UNIVERSIDAD VERACRUZANA

FACULTAD DE INGENIERIA EN ELECTRONICA Y COMUNICACIONES

REGION POZA RICA - TUXPAN

IMPLEMENTACION DE REDES DE AREA LOCAL VIRTUALES EN UN SWITCH MARCA CISCO MODELO 2950

TRABAJO PRÁCTICO EDUCATIVO

QUE PARA OBTENER EL TITULO DE:

INGENIERO EN ELECTRONICA Y COMUNICACIONES

PRESENTA:

DEIVI CESAREO FLEURY VICENCIO

ASESOR

ING. RAFAEL A. MORALES PULIDO

POZA RICA DE HGO., VER. **JUNIO DE 2007**

Índice

CAPITULO 1 INTRODUCCION

1.1 Justificación…… 4

1.2 Objetivos…….. 5

1.3 Características y funciones esenciales ……5

1.4 Descripción de la estructura de trabajo ……..... 6

CAPITULO 2

2.1 Definición de VLAN ……... 11

2.2 Tipos de implementaciones …… 12

2.2.1 VLAN de puerto central …… 12

2.2.2 VLAN estáticas ……12

2.2.3 VLAN dinámicas …… 14

2.3 Ventajas de la segmentación VLAN ……..15

2.3.1 Control de broadcast ……17

2.3.2 Seguridad ……18

2.3.3 Flexibilidad y escalabilidad ……...19

2.4 Tipos de conexiones en una VLAN ……21

2.4.1 Enlaces de acceso …… 21

2.4.2 Enlaces troncales …….. 22

2.5 Etiquetado de trama ……23

2.6 Funcionamiento del switch 25

2.6.1 Conmutación simétrica y asimétrica ……26

2.6.2 Almacenamiento temporal de memoria …… 26

2.6.3 Métodos de conmutación ……... 27

2.6.4 Aprendizaje MAC …… 29

2.6.5 Filtrado de tramas …….. 32

2.7 Spanning Tree 33
2.7.1 Estados del protocolo STP 34
2.7.2 Elección del switch raíz 37
2.7.3 Conexión de redundancia 39
2.7.4 Mantenimiento de la conectividad 39
2.7.5 Modos y protocolos STP 40

CAPITULO 3

3.1 Introducción al sistema operativo 45
3.2 Estructura de comandos CLI 46
3.2.1 Modo usuario EXEC 48
3.2.2 Modo privilegiado EXEC 48
3.2.3 Modo de configuración global 49
3.2.4 Modo de configuración de control 50
3.2.5 Modo de configuración de interfaz 50
3.2.6 Modo de configuración de secuencia 50
3.2.7 Modos VLAN 51
3.2.8 Modo de configuración de línea 52
3.3 El sistema de ayuda del IOS 52
3.3.1 Ayuda relativa al contexto 55
3.3.2 Mensajes de error de consola 56
3.3.3 Historial de comandos 56
3.4 Funciones administrativas 59
3.4.1 Nombre del equipo 60
3.4.2 Mensajes 61
3.4.3 Ajuste de contraseñas 63
3.4.3.1 Enable secret y enable password 64
3.4.3.2 Console password 65

3.4.3.3 Telnet password 66

CAPITULO IV

4.1 Soporte de VLANs 71

4.2 Modos de asignación de puertos 71

4.3 Configuración de VLANs en el rango normal 73

4.3.1 Consideraciones generales 74

4.4 Opciones de configuración 75

4.4.1 Modo config – vlan 75

4.4.2 Modo vlan configuration 76

4.4.3 Guardar la configuración VLAN 76

4.4.4 Configuración VLAN predeterminada 78

4.5 Creación de una VLAN Ethernet 79

4.5.1 Configurar una VLAN en el modo config – vlan 79

4.5.2 Configurar una VLAN en el modo vlan configuration 83

4.6 Asignación de puertos de acceso estático a una VLAN 85

4.7 Configuración de VLANs en el rango extendido 89

4.7.1 Guía de configuración 90

4.7.2 Configurar una VLAN en el rango extendido 91

4.8 Verificando la configuración VLAN 93

4.9 Eliminar una VLAN 94

4.10 Comunicación entre VLANs 96

CAPITULO V

5.1 El enlace troncal 111

5.1.1 Funcionamiento del enlace troncal 112

5.2 El estándar 802.1 Q 114

5.3 configuración de una interfaz Ethernet como puerto troncal 116

CAPITULO VI APORTACIONES
6.1 Aportaciones ……..127
6.2 Conclusiones ……. 128

ANEXOS
A Referencia de comandos ……129
B Características de los switches Cisco serie 2950 …….. 137
C Descripción del protocolo VTP ……..147
D Respuesta a las preguntas de repaso …….. 163

Bibliografía

CAPITULO **I**

INTRODUCCION

Esta hoja fue dejada en blanco a propósito

Las LAN virtuales (VLANs) se han colocado recientemente como una de las soluciones tecnológicas incorporadas en los equipos para redes conmutadas ofrecidos por diversos fabricantes, tanto para aplicaciones de datos y de voz; principalmente IP.

Una de las principales razones que justifican el uso de esta tecnología es el rápido desarrollo de la conmutación LAN. A principios de la década de los 90s, los diseñadores de red empezaron a reemplazar los hubs por dispositivos multipuerto de mayor capacidad, con estos diseños, los equipos de capa 3 formaban el bakbone de la red y contenían el tráfico de broadcast. Cada red usaba solamente routers para la segmentación, cada segmento estaba compuesto regularmente entre 100 y 300 usuarios.

Con la introducción de nuevas tecnologías de conmutación, las empresas empezaron a dividir sus redes en segmentos más pequeños, incrementando de esta manera el ancho de banda por segmento. Los routers eran los encargados de contener todo el tráfico de broadcast que era propagado por todos los segmentos, los cuales ahora podían soportar hasta 500 usuarios o más. Sin embargo, el constante desarrollo de los switches permitía dividir los segmentos en más segmentos, con lo cual el rendimiento de la red dependía de la capacidad del los routers.

Como solución a está situación surge la tecnología de conmutación virtual para redes Ethernet, mejor conocida como VLAN (Virtual Local Area Network). Las VLANs representan una alternativa para separar dominios de broascast, ya que permiten a los switches realizar el filtrado de tramas y evitar su difusión por toda la red. La incorporación en los diseños de red de los switches en conjunto con esta tecnología, permite que cada segmento de red pueda estar formado de unos cuantos equipos, mientras que los dominios de broadcast pueden tener 1000 usuarios o más.

Con un diseño adecuado, las VLANs facilitan el traslado o reubicación de los equipos sin tomar en cuanta una nueva reconfiguración, sin la necesidad de realizar cambios en el cableado o en el diseño de la red.

1.1 Justificación

La justificación para realizar este trabajo práctico-educativo se fundamenta en los siguientes hechos:

- Los diseños de redes de área local actuales, requieren la implementación de capacidades avanzadas de red que permitan migrar hacia nuevas tecnologías.
- La tecnología de VLAN, es una manera económica y eficiente de agrupar usuarios de la red en grupos de trabajo virtuales, sin importar su ubicación física en la red.
- La tecnología VLAN proporciona las siguientes ventajas; reduce los costos de administración (relacionados con los desplazamientos, adiciones y cambios), brinda seguridad de grupo de trabajo y de red, y controla la actividad de broadcast.
- La configuración de redes locales virtuales es proporcionada por otros servicios de telecomunicaciones que además, permiten la integración de tráfico como la voz, datos y video.
- Por lo anterior, aprender el proceso de implementar redes de área local virtuales, se convierte en una labor de suma importancia para implementar redes de datos.

En base en lo anterior, se presenta este trabajo que servirá como material didáctico que permita al personal académico, estudiantil y profesional, disponer de la información necesaria para realizar e interpretar

de manera adecuada la configuración de dicha tecnología en los equipos antes mencionados.

1.2 Objetivos

Objetivo general

- El propósito general de este trabajo, es apoyar el aprendizaje a través de la descripción del proceso de configuración de redes de área local virtuales (VLANs) en switches Cisco serie 2950.

Objetivos particulares

- Aumentar los conocimientos en la configuración de switches Cisco.
- Desarrollar una serie de ejercicios para explicar paso a paso el proceso de configuración.

1.3 Características y funciones principales

La función principal de este trabajo es desarrollar en su contenido los temas relacionados con el proceso de configuración antes mencionado. De tal manera que permitan al lector encontrar respuesta a los cuestionamientos y consideraciones que surgen cuando se transporta al ambiente práctico la teoría proporcionada por las guías de configuración, en este caso, la guía de configuración de los switches catalyst de la serie 2900. Estos equipos se encuentran en el laboratorio de prácticas del Programa CCNA (Cisco Networking Academy) impartido en la Facultad de Ingeniería en Electrónica y Comunicaciones.

Para tomar un enfoque educativo se incluyen un conjunto de prácticas seleccionadas en relación al contenido de cada capitulo, las cuales incluyen una serie de preguntas de repaso y prácticas de laboratorio con la finalidad de que el lector reafirme la comprensión de los temas propuestos.

En la estructura temática del trabajo se incluye la parte teórica que está directamente relacionada con cada paso del proceso de configuración descrito, con esto se dará una mejor comprensión de los conceptos.

1.4 Descripción de la estructura del trabajo

En el capítulo I se describen las ventajas que ofrece la conmutación VLAN respecto a la segmentación tradicional (LAN), a si como también los métodos utilizados para su implementación.

Se describe además, el mecanismo de transporte de las VLAN a través de los backbones de la red, lo cuál permite el flujo de información de los usuarios finales, identificación entre switches, routers y servidores directamente conectados.

En el capítulo III encontrará información acerca de las funciones y aplicaciones de los comandos más utilizados, no solo para realizar la configuración de la VLAN, si no también para llevar a cabo la administración del switch. Con la finalidad de reafirmar los conocimientos adquiridos en este capitulo, se incluye un cuestionario y prácticas de laboratorio.

En el capítulo IV se concentra el objetivo principal de este trabajo. Es decir, describir paso a paso el proceso necesario para realizar la configuración VLANs en el switch. Aquí se mencionan todos los criterios y consideraciones que se deben tomar en cuenta al momento de configurar una VLAN. Al final se incluye un cuestionario y prácticas de laboratorio para asegurar los conocimientos adquiridos.

El capítulo V está dirigido a explicar el papel que desempeñan los enlaces troncales en una red conmutada. Así como también, describir como estos enlaces permiten transportar tráfico de dos o más VLANs. Además, con

la finalidad de permitir una mejor administración de la red virtual implementada en el switch, se describe el proceso de configuración del protocolo de enlace troncal (VLAN Trunking Protocol, VTP), el cuál permite mantener una configuración coherente en la red. Al igual que en los capítulos anteriores se incluye un cuestionario y prácticas de laboratorio para que el lector ponga a prueba los conocimientos adquiridos En el capítulo VI se explican las aportaciones educativas proporcionadas a lo largo de la estructura de este trabajo práctico educativo.

CAPITULO

II

CONCEPTOS DE REDES DE AREA LOCAL VIRTUALES

2.1 Definición de VLAN

Una VLAN es una red conmutada que está segmentada lógicamente por función, equipo de proyecto o aplicación, sin tener en cuenta la ubicación física de los usuarios en la red. Las VLAN tienen los mismos atributos que una LAN física, pero podemos agrupar estaciones finales que no estén físicamente localizadas en el mismo segmento LAN.

Cualquier puerto del switch que pertenezca a una VLAN puede enviar paquetes unicast, broadcast y multicast e inundar solo a las estaciones finales que pertenezcan a dicha VLAN. Cada VLAN es considerada como una red lógica, por tanto, los paquetes destinados a estaciones que no pertenezcan a la misma VLAN deben ser enrutados a través de un router o bridge, tal como se muestra en la figura 2.1.

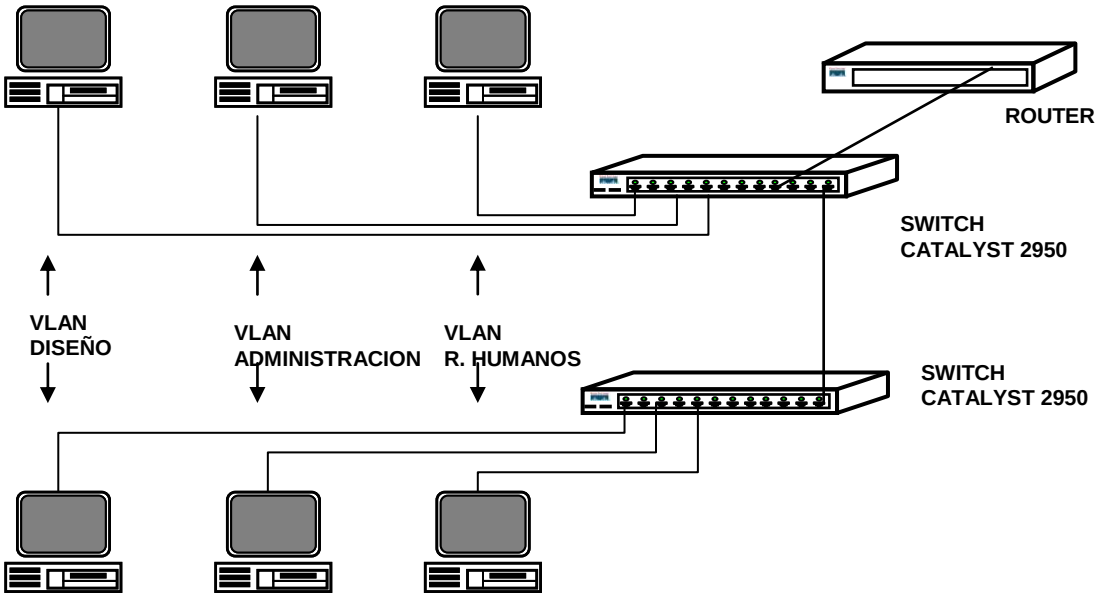


Figura 2.1 Red formada por VLANs

Una VLAN es asociada frecuentemente con subredes IP. Por ejemplo, todas las estaciones con una subred IP particular pertenecen a la misma VLAN.

2.2 Tipos de Implementaciones.

Las VLANs son creadas por el administrador de la red, quien determina los puertos del switch que serán asignados a cada VLAN. Cuando la asignación de los puertos se realiza en forma manual, tales VLANs son llamadas ***VLANs estáticas***. Si el administrador quiere reducir el trabajo que representa asignar las direcciones de hardware a cada host, los switch pueden ser configurados para asignar VLAN dinámicamente a los host que sean conectados al switch. Cuando la configuración se realiza de esta manera, estas VLAN son llamadas ***VLANs Dinámicas***.

2.2.1 VLAN de puerto central

En las VLAN de puerto central, todos los nodos conectados a puertos en la misma VLAN se les asignan el mismo identificador (ID) de VLAN. La figura 2.2 muestra la pertenencia a la VLAN por puerto, lo que facilita el trabajo del administrador y hace que la red sea más eficiente por las razones siguientes:

- Los usuarios se asignan por puerto.
- Las VLAN son de fácil administración.
- Proporciona mayor seguridad entre las VLAN.
- Los paquetes no se "filtran" a otros dominios.

2.2.2 VLAN Estáticas

Las VLAN estáticas son el modo más usual para crear redes de área local virtuales, y estas son también las más seguras. Los puertos del switch que

son asignados a cierta VLAN, mantienen su configuración hasta que el administrador modifica manualmente la asignación.

Este tipo de configuración es más fácil de implementar y monitorear. A demás, el trabajo de administración generado por el movimiento de los usuarios en la red es fácilmente controlado. Aunque no debe descartar la posibilidad de utilizar algún software de administración de redes para la asignación de los puertos.

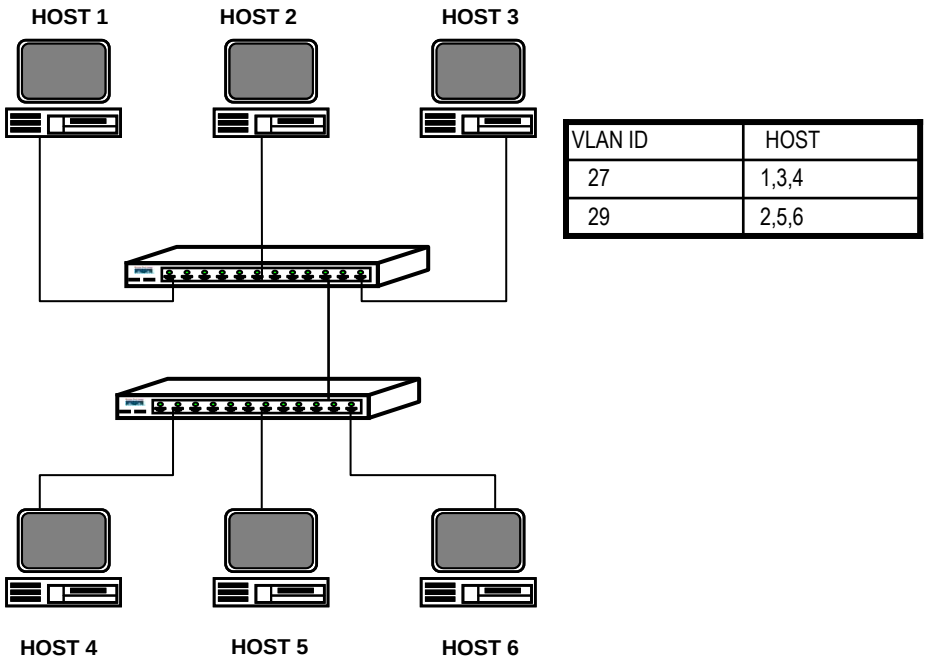


Figura 2.2 Los puertos pertenecientes a la misma VLAN se identifican con el mismo ID

En la figura 2.3, cada puerto del switch ha sido configurado con una membresía VLAN. Tomando en cuenta que cada host conectado debe ser miembro de alguna VLAN, la ubicación física del dispositivo no importa. Los dominios de broadcast se harán a los miembros que han sido administrativamente seleccionados.

Las VLANs forman subredes IP, por lo que cada host debe tener una correcta información de direccionamiento IP. Por ejemplo, cada host en la VLAN 2 debe ser configurado dentro de la red 172.16.20.0/24. Si conecta un host a un switch, debe verificar la membresía VLAN del puerto; si es diferente a la del host, este no será capaz de alcanzar los servicios de red que necesite.

IDENTIFICADOR	NOMBRE	SUBRED
VLAN 2	Ingeniería	196.10.68.0/27
VLAN 3	Finanzas	196.10.68.32/27
VLAN 4	Mercadotecnia	196.10.68.64/27

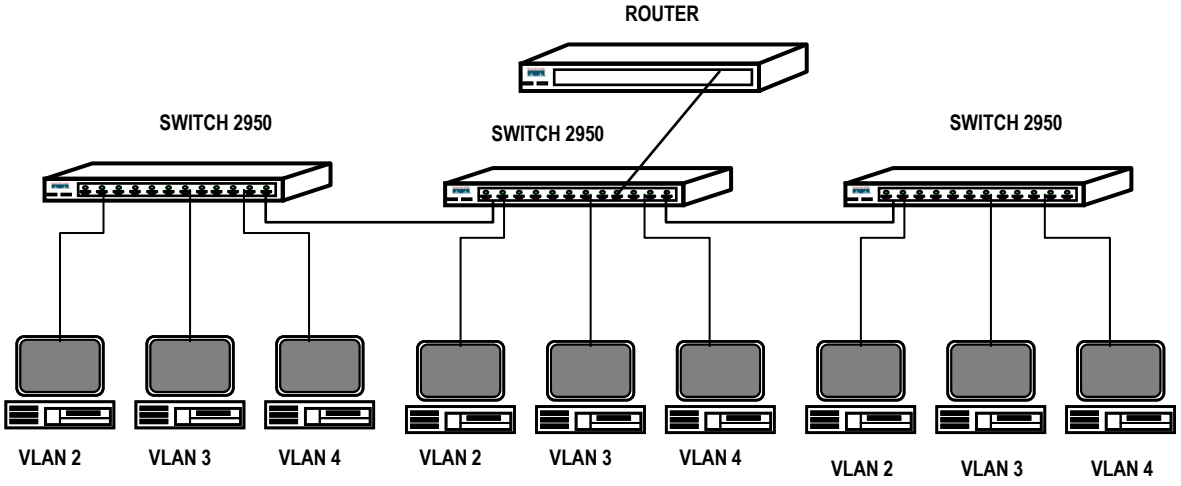


Figura 2.3 Propagación de VLANs a través de la red.

2.2.3 VLAN dinámicas

En una VLAN dinámica la asignación de puertos o membresías VLAN se realiza de manera automática. Con el uso de software inteligente de

administración de redes puede condicionar la asignación VLAN en base a direcciones de hardware, protocolo (IP, IPX), o aplicación.

Si un host es enganchado a un puerto no asignado, la base de datos de administración VLAN puede ver la dirección física asignada y configurar el puerto para una VLAN correcta. Esto hace muy fácil la administración y la configuración para el caso de usuarios móviles, ya que el switch asignará la VLAN correcta automáticamente.

2.3 Ventajas de la segmentación VLAN

Como se muestra en la figura 2.4, una red con conmutación de capa 2 es designada como una red plana. Debido a que los switches envían broadcast a todos los segmentos, cada paquete broadcast transmitido es visto por todos los dispositivos de la red sin consultar si el dispositivo receptor necesita recibir los datos.

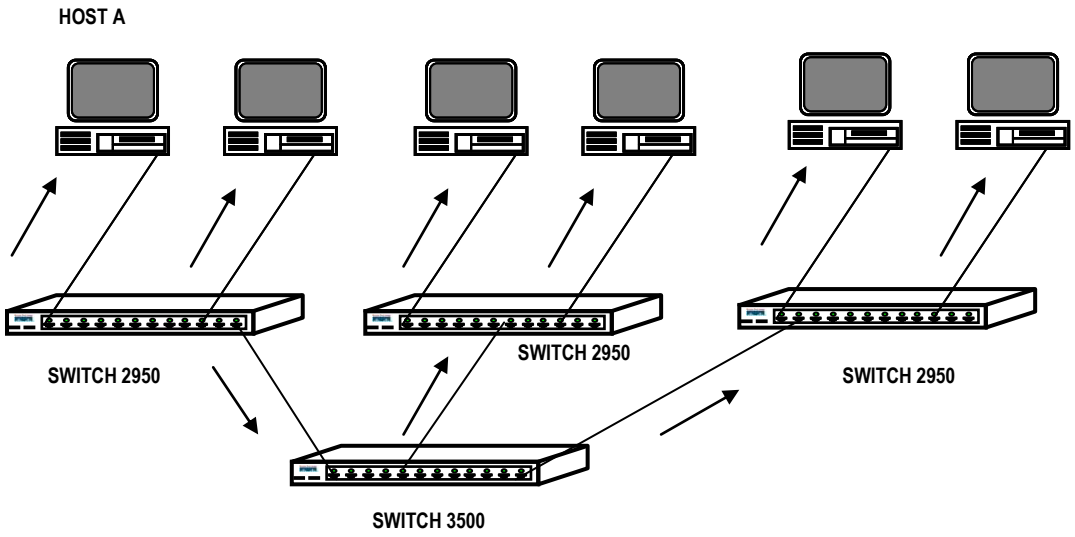


Figura 2.4 Estructura de una red plana

La figura 2.4 muestra que el host A envía un broadcast y todos los puertos de los switches reenvían este paquete; a excepción del puerto que originalmente lo recibió. Ahora observe la figura 2.5, esta muestra al host A enviando una trama con destino al host D, y como puede obervar, la trama solo es enviada por el puerto donde se localiza el host D, lo cual representa una enorme mejora en el rendimiento de la red. Esta figura permite conocer los beneficios que proporciona la conmutación de capa 2, la cual crea dominios de colisión individuales para cada dispositivo conectado en algún puerto del switch. Este ambiente elimina las restricciones Ethernet impuestas por la distancia y permite construir redes más extensas. Sin embargo, uno de los problemas potenciales en una red conmutada por capa 2 es la seguridad, estos problemas se presentan debido a la que la difusión de los paquetes es vista por todos los dispositivos en la red. En una red LAN las opciones de seguridad se limitan a passwords en los servidores y otros equipos.

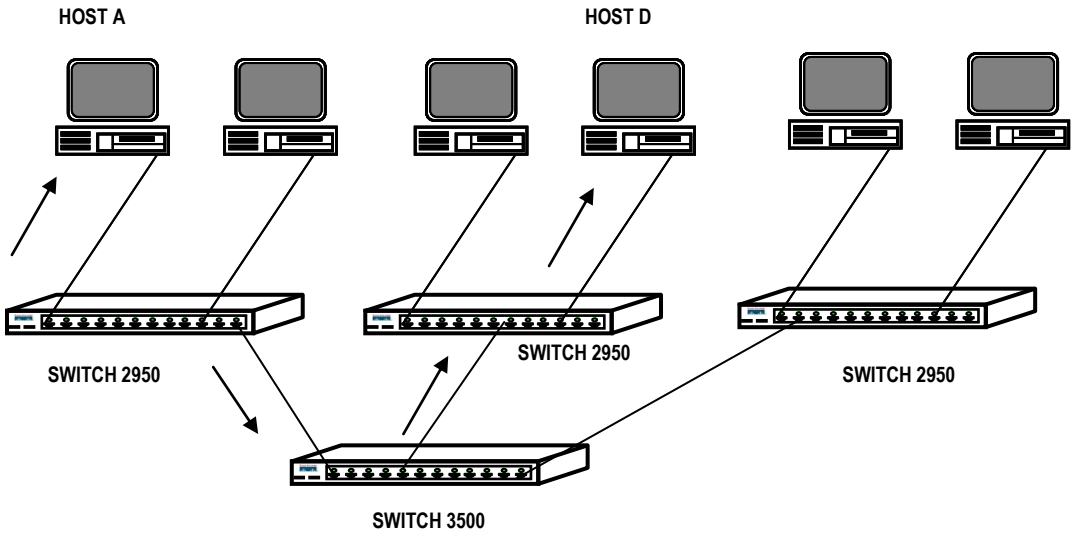


Figura 2.5 Una red conmutada mejora el desempeño de la red

Lo anterior no sucede al crear VLANs, se pueden resolver muchos de los problemas asociados con la conmutación de capa 2, principalmente aquellos que afectan la seguridad de la red.

Las VLANs ofrecen muchas ventajas que simplifican la administración de la red, de manera general pueden resumirse en las siguientes:

1. Las adiciones, traslados y cambios en la red, se logran configurando un puerto del switch en la VLAN adecuada.
2. Como los usuarios están agrupados lógicamente, las VLANs pueden implementarse independientemente de la localización física y geográfica de estos.
3. Las VLAN incrementan la seguridad de la red.
4. Las VLANs incrementan el número de dominios de broadcast mientras reducen su tamaño.

2.3.1 Control de Broadcast

Los broadcast ocurren prácticamente en cada protocolo, pero su aparición depende de tres factores:

1. El tipo de Protocolo.
2. El tipo de aplicación que se ejecute en la red.
3. El uso del servicio.

Las nuevas aplicaciones consumen gran parte del ancho de banda que encuentran por la red. Este abuso de ancho de banda es generado por aplicaciones multimedia que utilizan considerables paquetes broadcast y multicast. Equipo defectuoso, segmentación inadecuada y firewalls mal diseñados solo sirven para incrementar los problemas que ocasiona el uso intensivo de estas aplicaciones. Todo esto añade una nueva dimensión al diseño de la red y genera nuevos desafíos para el administrador. Un diseño

de red seguro que ofrezca una segmentación adecuada, y además, permita aislar los problemas en un segmento y mantener estos problemas fuera de la propagación de la red, resulta imprescindible.

La manera más efectiva de hacer esto es a través de una estrategia adecuada de conmutación y ruteo. Desde que los switches aumentaron sus capacidades de red, las compañías remplazaron sus redes planas con ambientes VLAN. Todos los dispositivos en una VLAN son miembros del mismo dominio de broadcast. Por defecto, los paquetes son filtrados para todos los puertos del switch que no sea miembro de la misma VLAN. Este es uno de los grandes beneficios que ofrece la segmentación VLAN, ya que los usuarios no tienen que preocuparse por los problemas de difusión, debido a que sus iguales están en el mismo dominio.

Este tipo de configuración reduce el tráfico total de broadcast, libera el ancho de banda para el tráfico real de usuarios, y reduce la vulnerabilidad general de la red a las tormentas de broadcast. Las VLAN son un mecanismo efectivo para extender los firewalls desde los routers a la estructura de los switches y proteger la red contra problemas de broadcast.

2.3.2 Seguridad

La seguridad de los equipos interconectados en una red interna plana, se logra conectando los hubs y switches a un router. Este arreglo es bastante inadecuado por varias razones. Primera, cualquier equipó que se conecte a la red física puede acceder a los recursos localizados en la LAN. Segunda, todos los equipos conectados pueden ver todo o parte del tráfico que circule por la red. Y tercera, los usuarios pueden trabajar en grupos simplemente conectando sus estaciones en el hub existente. Así, básicamente este arreglo no proporcionaba seguridad.

Una técnica de administración económica y sencilla para aumentar la seguridad, consiste en segmentar la red en múltiples grupos de broadcast que permitan al administrador de red:

1. Limitar la cantidad de usuarios en un grupo de VLAN.
2. Evitar que determinado usuario se conecte en algún puerto no asignado
3. Configurar todos los puertos no utilizados en una VLAN de bajo servicio.

La construcción de VLANs permite crear múltiples grupos de broadcast, y esto permite al administrador tener control de cada puerto y por lo tanto de cada usuario. Por consiguiente, se eliminan las posibilidades de que un usuario conecte su estación a algún puerto de switch y obtenga acceso a los recursos de la red. El administrador es ahora quien concede el acceso a cada puerto y a cualquier recurso en la red.

Las VLAN pueden ser creadas en base a los recursos que el usuario requiera, a demás, los switches pueden ser configurados para informar si una estación intenta acceder a los recursos de la red en un puerto no autorizado. Si necesita comunicación inter-VLAN puede implementar restricciones en el router, tales restricciones pueden establecerse de acuerdo a la dirección física, protocolo y aplicación.

2.3.3 Flexibilidad y escalabilidad

Al implementar VLANs, crea pequeños dominios de broadcast, los broadcast enviados fuera del nodo (VLAN) no serán difundidos hacia los puertos configurados en diferentes VLANs. Asignando los puertos del switch en grupos VLAN o en un grupo de switches, gana flexibilidad para añadir solamente los usuarios que quiera dentro de un dominio de broadcast, sin

tener en cuenta su ubicación física. Está implementación permite a la red funcionar pese a las tormentas de broadcast causadas por alguna NIC defectuosa. Tanto como que un dispositivo propagué tormentas de difusión a lo largo de la red interna.

Para comprender como son vistas las VLAN por el switch, es útil empezar primero por analizar una red tradicional. La figura 2.6 muestra una red que ha sido creada conectando switches (LAN físicas) y routers.

En esta figura puede ver que cada red ha sido conectada a un puerto del router, cada nodo conectado a una red física particular, posee una dirección lógica que le permite tener comunicación en la red interna. Note que cada departamento forma una LAN, si desea añadir nuevos usuarios al área de ventas, por ejemplo, tendrá que conectarlos en dicha VLAN (VLAN de ventas) para que formen parte del mismo dominio de broadcast.

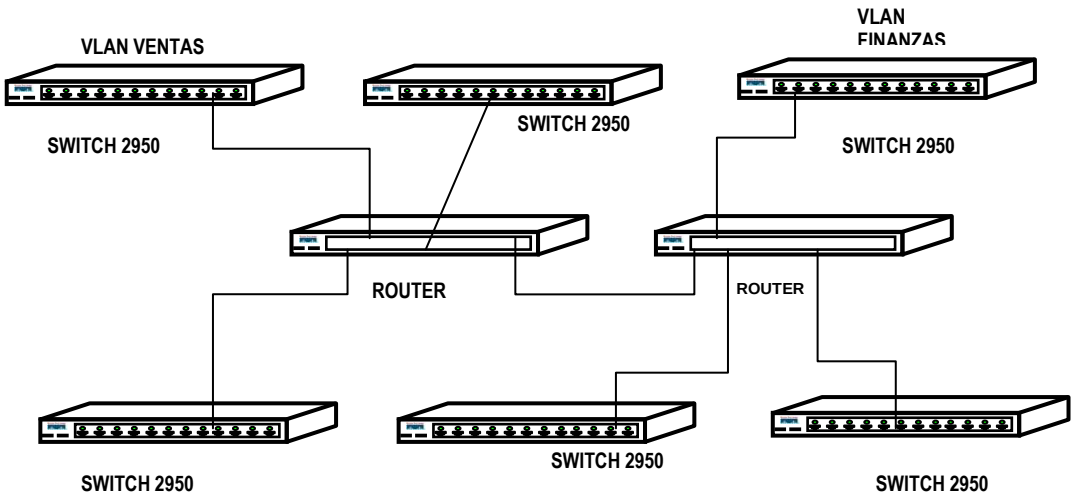


Figura 2.6 LANs físicas conectadas medio de routers

Pero, que sucede si el hub de ventas no tiene puertos disponibles y necesita agregar otro usuario en la LAN de ventas. Y además, el lugar donde se encuentra ubicado el equipo de ventas carece de espacio para agregar otro empleado. Supongamos que el hub en la LAN de Finanzas cuenta con espacio y puertos disponibles para instalar más usuarios. Para solucionar este problema, la única opción es conectar el nuevo empleado de ventas en esta LAN.

Al realizar esta configuración, el nuevo usuario será parte de la LAN de Finanzas, lo cuál es muy malo por muchas razones. La primera y principal, representa un problema de seguridad, esto a causa de que el nuevo usuario es parte del dominio de broadcast de finanzas y puede por lo tanto, acceder a todos los servicios de esta red. Segunda, para que este usuario pueda utilizar los recursos de la red de ventas, necesita una conexión a través del router.

La figura 2.3 muestra como los switches eliminan los límites físicos para solucionar el problema. Las VLANs numeradas del 2 al 4 se usan para crear dominios de broadcast en cada departamento. Cada puerto del switch es asignado con una membresía. De esta manera, si es necesario agregar otro usuario a la VLAN de ventas, solo se debe configurar el puerto para que pertenezca a esta VLAN. Sin tener en cuenta la ubicación del nuevo miembro del equipo de ventas.

Como se puede ver en la figura 2.3, los identificadores para cada VLAN inician a partir del Número 2, esto se debe a que la VLAN 1 se encuentra reservada para propósitos de administración y todos los puertos del switch serán miembros de esta VLAN hasta que sean asignados a otra VLAN o sean cambiados del grupo de administración.

2.4 Tipos de conexiones en una VLAN

Como las tramas son conmutadas a través de la red, los switches deben ser capaces de trasportarlas en base a la dirección física asignada. Las tramas son transportadas de acuerdo al tipo de conexión por la cuál viajan.

Existen dos tipos diferentes de conexión en un ambiente conmutado, estos métodos se describen en la siguiente sección.

2.4.1 Enlaces de acceso

Estos tipos de enlaces solo son parte de una VLAN, los dispositivos conectados asumen que pertenecen a un dominio broadcast, pero estos no conocen la red física.

Los switches eliminan cualquier trama antes de ser enviada a otro dispositivo por el enlace de acceso. Los host con este tipo de conexión no pueden comunicarse con otros host que estén fuera de su VLAN a menos que el paquete sea enrutado.

2.4.2 Enlaces troncales

Los enlaces troncales pueden llevar múltiples VLANs y deben su nombre al sistema de troncales telefónicas que pueden transportar múltiples conversaciones telefónicas. Un enlace troncal es una conexión punto a punto de 100 a 1000 Mbps entre dos switches, entre un switch y un router o entre un switch y un servidor, que puede transportar tráfico de diversas VLANs en un instante de tiempo.

En una conexión entre switches, los enlaces troncales pueden transportar toda la información VLAN sobre el enlace. Pero si este enlace

entre los switches no se define como un enlace troncal, solo la información de la VLAN 1 será transportada a través del puerto.

La figura 2.7 muestra como los diferentes enlaces son usados en una red conmutada. Debido al enlace troncal que existe entre estos switches, todos los host conectados a los switches pueden comunicarse a todos los puertos en sus respectivas VLAN.

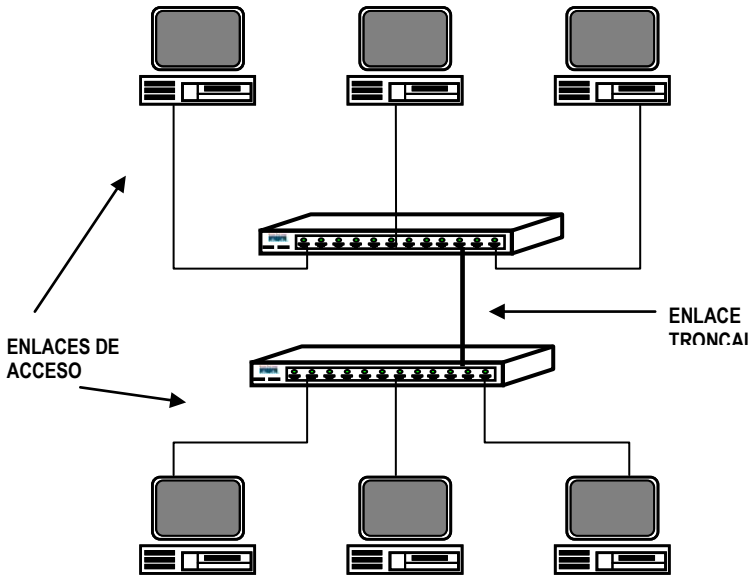


Figura 2.7 Los enlaces troncales proporcionan comunicación en la red

El estándar de etiquetado requiere de un solo Spanning Tree (STP) para todas las VLAN permitidas en el enlace troncal. Sin embargo, en una red de switches Cisco conectados a través de un enlace troncal IEEE 802.1Q, los switches mantienen un STP para cada VLAN permitida sobre el enlace troncal.

Cuando interconecta un switch Cisco a otro switch de diferente fabricante mediante el estándar troncal, el switch Cisco utiliza Per Spanning Tree Plus (PVST+) para proporcionar interoperabilidad. Si el rapid PVST+ esta habilitado, el switch lo utiliza en lugar de PVST+. El switch combina el

ejemplo spanning tree de la VLAN 802.1Q del enlace del switch Cisco con el spaning tree del otro dispositivo.

Sin embargo, los switch Cisco mantienen la información de PVST+ y del rapid PVST+ separada de los otros equipos, los cuales son tomados como una nube separada. Esta nube es tratada como una solo conexión entre los demás switches.

2.5 Etiquetado de trama

Como se ha visto hasta ahora, puede crear redes de área local virtuales mediante switches conectados y transportar el tráfico a través de un enlace troncal. En la figura 2.3, host de varias VLAN pueden difundir tramas a través de muchos switches, esta capacidad es probablemente la ventaja principal de implementar VLANs. Pero este proceso podría complicarse, regularmente el switch necesita mantener una trayectoria para cada una de las tramas de todos los usuarios que sean miembros de una VLAN.

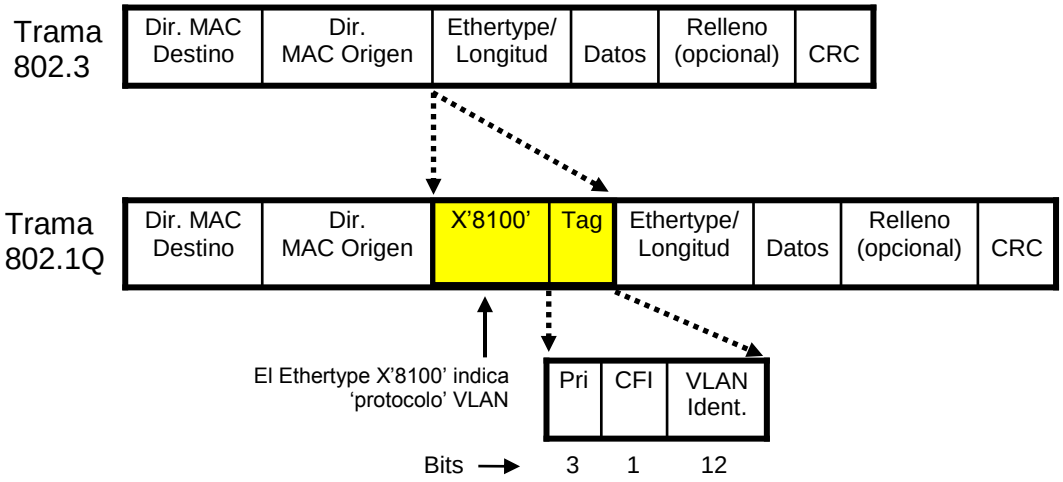
Aquí es donde entra el etiquetado de trama, este método de identificación únicamente asigna un identificador “ID” a cada trama, normalmente conocido como *VLAN ID*. Cada switch debe identificar primero el *VLAN ID* en el encabezado de trama, y entonces decidir que hacer con la trama consultando la información en su tabla de filtrado. Si la trama está dirigida a otro switch que esté conectado por medio de un enlace troncal, la trama será enviada por el puerto que tenga esa conexión.

La identificación VLAN es el mecanismo que utilizan los switches para identificar cuál trama pertenece a cierta VLAN y tomar la decición de envío por la red. Existen dos métodos de etiquetado de trama:

1. ***Inter-Switch Link (ISL).*** Este es un protocolo propietario de Cisco y es usado solamente para conexiones Fast Ethernet y Gigabit Ethernet.

El enrutamiento ISL puede ser usado sobre puertos de switch, interfaces de routers y tarjetas de interfaz para un servicio troncal.

2. ***IEEE 802.1Q.*** Creado por el IEEE como un método estándar para el etiquetado de trama. La figura 2.8 muestra el formato de trama establecido por el IEEE, en la cual se inserta un campo para identificar la VLAN. Si realiza un enlace troncal entre un switch cisco y un switch de otro fabricante, puede utilizar este método de etiquetado.



Pri: Prioridad (8 niveles posibles)
CFI: Canonical Format Indicator (indica formato de direcciones MAC)
VLAN Ident.: Identificador VLAN (máximo 4096 en una misma

Figura 2.8 Formato de trama 802.1 Q

Puede configurar cada puerto con el estándar 802.1Q y asociarlo con un *VLAN ID* específico. Todos los puertos asignados crearán un grupo conocido como *VLAN por defecto* y cada puerto obtendrá una etiqueta con un número de identificación que representará su VLAN. En el capítulo 5, se describen con un mayor detalle estos métodos de identificación.

2.6 Funcionamiento del switch

La conmutación es una tecnología que reduce la congestión en las redes de área local disminuyendo el flujo de tramas y aumentando el ancho de banda. Los switches LAN se utilizan frecuentemente para reemplazar hubs compartidos. Están diseñados para funcionar con infraestructuras de cableado existentes, de manera que pueden instalarse sin provocar disturbios en la red existente.

Actualmente, en la comunicación de datos todos los equipos de conmutación realizan dos operaciones básicas:

a) Conmutación de tramas de datos. Está ocurre cuando una trama llega por un medio de entrada y se transmite por un medio de salida.
b) Mantenimiento de las operaciones de conmutación. Un switch desarrolla, mantiene y actualiza tablas de conmutación.

Como se ha descrito en las secciones anteriores, las redes de área local virtuales mejoran en muchos aspectos la funcionalidad de la red. Aún con el agrupamiento lógico de los usuarios (o host) sin considerar su ubicación física, las VLAN comparten algunas características de una red LAN, entre las que sobresale el direccionamiento de capa 2 (capa de enlace de datos del modelo OSI).

En ambas implementaciones (LANs y VLANs) la conmutación de capa 2 la proporciona el dispositivo de conmutación, es decir, el switch. El método que utiliza un switch para realizar la conmutación de las tramas hacia la VLAN correcta es el mismo, por lo que resulta sumamente importante conocer el funcionamiento de estos equipos.

Las secciones siguientes están dirigidas a ofrecer una descripción del funcionamiento del switch, a si como también, explicar todos los conceptos

que envuelven el proceso de conmutación que realizan estos dispositivos, generalmente conocido como **switching.**

2.6.1 Conmutación simétrica y asimétrica.

La conmutación se clasifica en base al ancho de banda asignado a cada puerto. Un switch simétrico proporciona conexiones conmutadas entre puertos con el mismo ancho de banda, por ejemplo, puertos de 10 Mbps o 100 Mbps. En cambio un switch asimétrico proporciona conexiones conmutadas entre puertos con distinto ancho de banda, por ejemplo, una combinación de puertos de 10 Mbps y de 100 Mbps.

La conmutación asimétrica permite que la mayor parte del tráfico de red (por lo regular cliente/servidor) fluya donde múltiples clientes se comunican con un servidor al mismo tiempo, en este ambiente se necesitará asignar más ancho de banda dedicado al puerto del switch al cual está conectado el servidor, con la finalidad de evitar el cuello de botella en este puerto. Se requiere un búfer de memoria en un switch asimétrico para permitir que el tráfico del puerto de 100 Mbps, pueda enviarse al puerto de 10 Mbps sin provocar congestión en el puerto de 10 Mbps.

2.6.2 Almacenamiento temporal de memoria

Un switch Ethernet utiliza el método de almacenamiento temporal de memoria (búfer) para almacenar y enviar paquetes a los puertos correctos. El búfer también puede utilizarse cuando el puerto destino está ocupado. El área de la memoria en la que el switch almacena los datos se denomina "búfer de memoria". Este búfer de memoria puede utilizar dos métodos para enviar paquetes: el búfer de memoria basado en puerto y el búfer de memoria compartida.

En el búfer de memoria basado en puerto, los paquetes se almacenan en colas enlazadas a los puertos de entrada específicos. Un paquete se

transmite por el puerto de salida una vez que todos los paquetes que están delante de éste, se hayan transmitido con éxito. Es posible que un solo paquete retarde la transmisión de todos los paquetes almacenados en la memoria. Este retardo se produce aún si los demás paquetes se pueden transmitir a los puertos destino abiertos.

El búfer de memoria compartida deposita todos los paquetes en un búfer de memoria común que comparten todos los puertos del switch. La cantidad de memoria asignada a un puerto se determina según la cantidad que cada puerto requiere, esto se denomina *asignación dinámica de la memoria del búfer*. Los paquetes en el búfer se enlazan dinámicamente al puerto de transmisión, lo cual permite recibir el paquete en un puerto y transmitirlo a otro puerto, sin tener que colocarlo en otra cola.

El switch conserva un mapa de los puertos a los cuales un paquete debe ser transmitido, el switch despeja este mapa de puertos destino sólo después de que el paquete se haya transmitido con éxito. Como el búfer de memoria se comparte, se restringe el paquete según el tamaño del búfer. Esto significa que las tramas más grandes se pueden transmitir con menos tramas descartadas. Esto es importante para la conmutación 10/100, donde un puerto de 100 Mbps puede enviar una trama a un puerto de 10 Mbps.

2.6.3 Métodos de conmutación

El proceso de conmutación consiste en tomar una trama que ingresa por un puerto y transmitirla por otro puerto hacia su destino. El switch utiliza dos modos de conmutación para enviar una trama, estos modos de conmutación se describen a continuación:

1. **Almacenamiento y envío**. La trama completa se recibe antes de que se realice cualquier tipo de envío. El switch examina las direcciones destino y origen, y aplica filtros antes de enviarla. Se produce latencia mientras se recibe la trama; la latencia es mayor con tramas más

grandes, debido a que la trama completa tarda más en leerse. La detección de errores es alta debido al tiempo disponible para que el switch verifique los errores, mientras espera la recepción de la trama completa.

2. **Método de corte**. El switch lee la dirección destino antes de recibir la trama completa. La trama luego comienza a ser enviada antes de que ésta llegue completamente. Este modo reduce la latencia de la transmisión, pero la detección de errores es mínima. Existen dos formas de conmutación de método de corte; conmutación rápida y libre de fragmentos.

   a) Conmutación rápida Este método de conmutación ofrece el nivel de latencia más bajo, al enviar inmediatamente un paquete luego de recibir la dirección destino. Como la conmutación rápida empieza a realizar el envío antes de recibir el paquete completo, de vez en cuando los paquetes se pueden entregar con errores. Aunque esto se produce con muy poca frecuencia, el adaptador de red destino descarta el paquete defectuoso en el momento de su recepción. Utilice la opción libre de fragmentos para reducir la cantidad de paquetes enviados con errores. En el modo rápido, la latencia se mide desde el primer bit recibido al primer bit transmitido, o bien, el primero en entrar y el primero en salir (FIFO).

   b) Conmutación libre de fragmentos La conmutación libre de fragmentos filtra los fragmentos de colisión, que constituyen la mayoría de los errores en los paquetes antes de iniciar el envío. En una red que funciona correctamente, los fragmentos de colisión deben ser mayores de 64 bytes. Cualquier datagrama superior a 64 bytes es un paquete válido y se recibe generalmente sin errores. La conmutación libre de fragmentos determina si el paquete no es un fragmento de colisión antes de enviar dicho paquete. En el modo libre de fragmentos, la latencia se mide como FIFO.

La latencia de cada modo de conmutación depende de la manera en que el switch envía las tramas. Cuanto más rápido sea el modo de conmutación, menor será la latencia dentro del switch. Para agilizar el envío de la trama, el switch dedica menos tiempo a la verificación de los errores. Como consecuencia, se reduce la verificación de errores, lo que puede llevar a aumentar la cantidad de retransmisiones.

2.6.4 Aprendizaje MAC

Los switches segmentan la red en diferentes dominios de colisión, aprenden direcciones lógicas, reenvian, filtran tramas y evitar loops. Segmentan el tráfico de manera que los paquetes destinados a un dominio de colisión no se propaguen a otro segmento.

El switch hace esto aprendiendo las direcciones lógicas de los host. Enviar una trama a todos los puertos conectados se denomina “inundar” la trama. Los switches controlan él trafico para múltiples segmentos y al mismo tiempo implementan memoria del búfer para que puedan recibir y transmitir tramas en cada puerto o segmento.

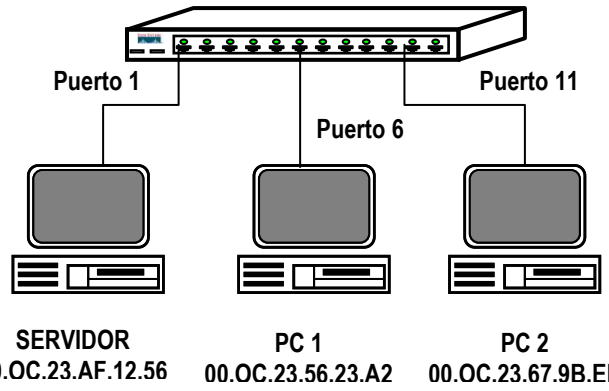
Leyendo la dirección origen de cada paquete transmitido y anotando el puerto de entrada de la trama, el switch puede aprender la dirección MAC de cada dispositivo en la red. El switch entonces agrega esta información a su base de datos de envío. Las direcciones se aprenden de forma dinámica. Esto significa que, a medida que se leen las nuevas direcciones, éstas se aprenden y se almacenan en una memoria de contenido direccionable (CAM). Cuando se lee un origen que no se encuentra en la CAM, se aprende y almacena para su uso futuro.

La dirección MAC (Media Access Control address) es un identificador hexadecimal de 48 bits, que es asociado de forma única con una tarjeta o interfaz de red. Es individual, cada dispositivo tiene su propia dirección MAC

determinada y configurada por el IEEE (los últimos 24 bits) y el fabricante (los primeros 24 bits). La mayoría de los protocolos que trabajan en la capa 2 del modelo OSI, utilizan una de las tres numeraciones manejadas por el IEEE: **MAC-48, EUI-48, y EUI-64.**

Cada vez que una dirección se almacena, se le agrega una marca horaria. Esto permite almacenar las direcciones durante un tiempo determinado. Cada vez que se hace referencia a una dirección que se encuentra en CAM, recibe una nueva marca horaria. Las direcciones que no son utilizadas se eliminan de la lista. Al eliminar direcciones antiguas, la CAM mantiene una base de datos de envío precisa y funcional.

Para comprender el aprendizaje MAC del switch consideremos la figura 2.9, la cuál muestra una red formada por dos host y un servidor conectados a los puertos de un switch.



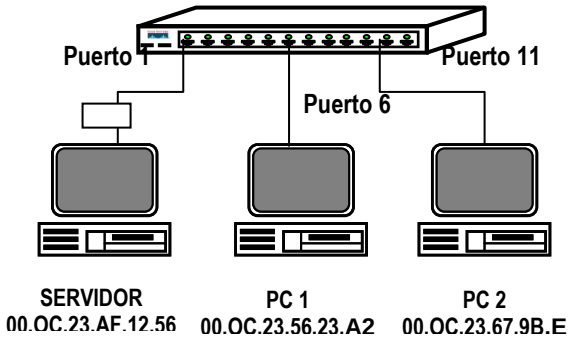
Puerto	Dirección
1	
6	
11	

Figura 2.9 Cuando el switch inicia su operación la tabla de direcciones se encuentra vacía

El proceso que ejecuta el switch para difundir tramas hacia los puertos correctos puede resumirse en los pasos siguientes:

1. Cuando el switch inicia su operación, la tabla está en blanco, figura 2.9.

2. Cuando el servidor envía una trama a la PC 2, el switch la reenvía a todos los puertos activos con excepción del puerto de origen, que en este caso es el puerto 1. El switch aprende la dirección MAC del servidor conectado al puerto y la configura en su tabla de direcciones, figura 2.10.

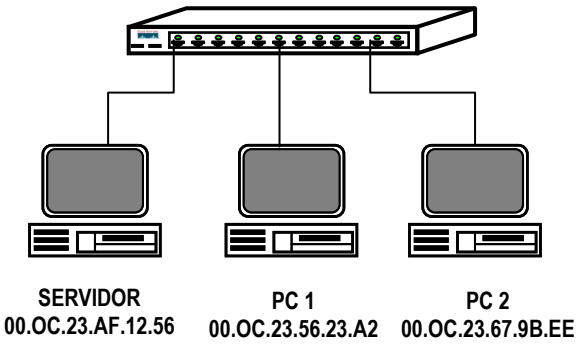


Puerto	**Dirección**
1	00.OC.23.AF.12.56
6	
11	

Figura 2.10 El switch aprende la dirección MAC del servidor y la configura en su tabla.

3. La trama contiene la dirección MAC origen y destino, si el host destino esta conectado a algún puerto activo del switch, confirmará a esté que la dirección destino corresponde a su dirección física, y el switch reenviará la trama hacia el puerto correcto.

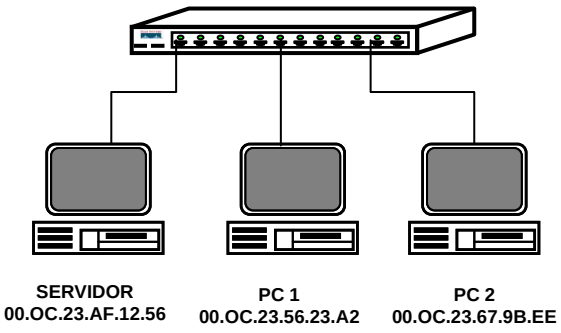
4. Cuando la PC contesta al servidor, el switch conoce la ubicación de esta dirección y envía la trama exclusivamente al puerto 1, en donde está el servidor. El switch aprende la dirección MAC de la PC 2 y la configura en su tabla, figura 2.11.



Puerto	Dirección
1	00.OC.23.AF.12.56
6	
11	00.OC.23.67.9B.EE

Figura 2.11 El switch aprende la dirección MAC de la PC1 y la configura en su tabla

5. Una vez que todas las estaciones han transmitido, el switch completa su tabla, figura 2.12. Posteriormente, monitorea constantemente los puertos a fin de mantener actualizada su tabla. Si una dirección deja de verse en cierto tiempo, es eliminada de la tabla.



Puerto	Dirección
1	00.OC.23.AF.12.56
6	00.OC.23.56.23.A2
11	00.OC.23.67.9B.EE

Figura 2.12 Cuando todas las estaciones han transmitido el switch completa su tabla

2.6.5 Filtrado de tramas.

El switch no retransmite la trama nada más que al puerto especifico al que va dirigida, preservando el ancho de banda del resto de los enlaces. Las tramas de difusión y multidifusión constituyen un caso especial. Un switch nunca aprende direcciones de difusión o multidifusión, dado que las direcciones no aparecen en estos casos como dirección de origen de la trama.

Otra función del switches es evitar **loops**. Las redes están diseñadas por lo general con enlaces y dispositivos redundantes. Estos diseños eliminan la posibilidad de que un punto de fallo individual, origine al mismo tiempo varios problemas en la red. Sin esta característica los switches inundarían los puertos con difusiones múltiples ocasionando un loop infinito, llamado también loop de puente.

La propagación continúa de estas difusiones a través del loop produce una tormenta de difusión, dando como resultado un desperdicio del ancho de banda, así como impactos serios en el rendimiento de la red. Pueden distribuirse múltiples copias de tramas hacia los puestos destino, muchos protocolos esperan recibir una sola copia de cada transmisión. La presencia de múltiples copias de la misma trama causa inestabilidad en el contenido de la tabla de direcciones MAC, lo cual da como resultado que se reciban varias copias de una misma trama en diferentes puertos del switch.

2.7 Spanning Tree

Spaning Tree es un protocolo de tipo puente a puente desarrollado por Digital Equipment Corporation (DEC), revisado posteriormente por el IEEE y publicado en la especificación IEEE 802.1. El objetivo del protocolo de árbol de extensión es mantener una red libre de loops. Un camino libre de loops se consigue cuando un dispositivo es capaz de reconocer un loop en la topología de la red y bloquear uno o más puertos redundantes.

Los puentes y los switches toman sus decisiones de reenvió para tramas de unidifusión en base a la dirección MAC destino de la trama. Si la dirección MAC es desconocida, el dispositivo inundará la trama en todos los puertos en un intento de alcanzar el destino deseado.

El algoritmo Spanning Tree, implementado por el protocolo STP, impide los loops calculando una topología de red estable. Cuado se crean redes tolerantes a fallos, debe haber una ruta sin loops entre todos los nodos de la red. Las unidades de datos del protocolo de puente (BPDUs) son enviadas y recibidas por los switches a intervalos regulares, y se usan para determinar la topología Spanning Tree.

Los switches utilizan el protocolo STP en todas las VLAN basadas en Ethernet y Fast Ethernet. El protocolo separa y detecta los loops colocando algunas conexiones en modo de espera, las cuales se activan en caso de fallo en una conexión activa.

STP explora constantemente la red, de forma que cualquier fallo o adición de un enlace, switch o router es detectado al instante. Cuando cambia la topología de la red, el algoritmo reconfigura los puertos del switch para evitar una pérdida total de la conectividad creando una topología de red libre de loops, éste proceso lleva a cabo las operaciones siguientes:

1. **Elección de un Switch raíz.** En un dominio de difusión solo puede existir un switch raíz. Todos los puertos del switch raíz se encuentran en estado de retransmisión y se denominan puertos designados. Cuando el switch se encuentra en este estado, puede enviar y recibir tramas.
2. **Asignación de un puerto raíz.** El puerto raíz corresponde a la ruta de menor coste desde el switch no raíz, hasta el switch raíz. Los puertos raíz se encuentran en estado de retransmisión y proporcionan conectividad de retroalimentación al switch raíz. La ruta de menor coste al switch raíz se basa en el ancho de banda.
3. **Designación de puerto.** El puerto designado se selecciona en el switch que posee el trayecto de menor coste hacia el switch raíz. Los puertos designados se encuentran en estado de retransmisión y son los responsables del reenvío de tráfico por el segmento. Los puertos

no designados se encuentran normalmente en estado de bloqueo con el fin de romper la topología de loop.

2.7.1 Estados del protocolo STP

Un retraso en la propagación puede ocurrir cuando el protocolo converge a través de la red, como resultado la topología de la red cambia en tiempos y lugares diferentes. Cuando una interfaz pasa directamente al estado de reenvió y no pertenece a una topología de árbol puede crear loops de datos temporales. Las interfaces deben esperar que la información de la nueva topología se propague a través de la red antes que inicie el reenvió de las tramas en los switches.

Cuando da inicio el proceso de intercambio de BPDUs, los puertos pasan a través de los estados siguientes:

1. Del estado de Iniciación al bloqueo
2. Del bloqueo a escucha, o a inactivo
3. De escucha al aprendizaje, o a inactivo
4. De aprendizaje al reenvió, o a inactivo
5. Del reenvió a inactivo

La figura 2.13 muestra como una interfaz se traslada a través de los diferentes estados del protocolo. Cuando se enciende el switch, STP es habilitado por defecto en cada interfaz del switch, VLAN o red. Posteriormente pasa al estado de bloqueo para finalizar en el estado de escucha ó aprendizaje. STP estabiliza cada interfaz al estado de reenvió o bloqueo.

Cuando el algoritmo de STP ubica a una interfaz en el estado de reenvió ocurre el proceso siguiente:

1. La interfaz permanece en el estado de escucha mientras STP espera la información del protocolo para que la interfaz cambie al estado de bloqueo.
2. Mientras STP espera el intercambio de información, el tiempo de reenvió puede expirar, lo cual lleva a la interfaz al estado de aprendizaje y reajusta el contador de tiempo de reenvió.
3. En el estado de aprendizaje, la interfaz continúa bloqueada para el reenvió de tramas hasta que el switch aprenda la localización de la estación final y envié la base de datos.
4. Cuando el tiempo de reenvió de tramas expira, STP mueve la interfaz del estado de reenvió.

Las características de los estados por los que pasa cada interfaz se describen a continuación:

Estado de bloqueo. Una interfaz que se encuentra en el estado de bloqueo no participa en el envió de tramas. Después de iniciar, una BPDU (Unidad de Datos para Protocolo Puente) es enviada a cada interfaz del switch. Un switch funciona inicialmente como raíz hasta que intercambia BPDUs con otros switches. Este intercambio establece cuál switch en la red es el switch raíz. Si la red esta formada por un solo switch el intercambio no ocurre, el tiempo de envió de tramas expira y la interfaz pasa al estado de escucha. Una interfaz siempre pasa al estado de bloqueo después del proceso de inicio del switch y realiza lo siguiente:

1. Descarta las tramas recibidas en un puerto.
2. Descarta las tramas conmutadas hacia otra interfaz.
3. No aprende direcciones MAC.
4. Recibe BPDUs.

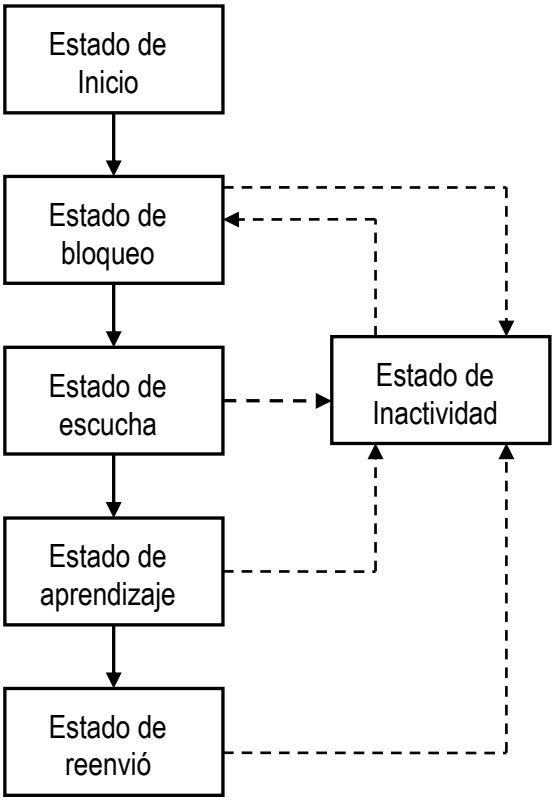


Figura 2.13 Estados del protocolo de árbol de extensión

Estado de escucha. El estado de escucha, es el primer estado al que pasa una interfaz después del bloqueo. La interfaz entra a este estado cuando Spanning Tree determina que la interfaz puede participar en el envió de tramas. Una interfaz en el estado de escucha realiza lo siguiente:

1. Descarta las tramas recibidas en un puerto.
2. Descarta las tramas conmutadas hacia otra interfaz.
3. No aprende direcciones.
4. Recibe BPDUs.

Estado de aprendizaje. La interfaz participa en el envió de tramas e ingresa al estado de aprendizaje desde el estado de escucha. Una interfaz que se encuentre en este estado, lleva a cabo las mismas tareas que los estados de bloqueo y escucha.

Estado de reenvió. La interfaz participa en el envió de tramas, pasa al estado reenvió desde el aprendizaje y realiza lo siguiente:

1. Envía las tramas recibidas en algún puerto.
2. Envía las tramas que han sido conmutadas desde otros puertos.
3. Aprende direcciones MAC.
4. Recibe BPDUs.

Estado inactivo. Una interfaz en el estado de inactividad no participa en el reenvió de tramas o en el algoritmo STP. La interfaz es inoperable y realiza lo siguiente:

1. Descarta las tramas recibidas en un puerto
2. Descarta las tramas conmutadas hacia otra interfaz
3. No aprende direcciones MAC
4. Recibe BPDUs

2.7.2 Elección del switch raíz

Si en una red VLAN, los switches tienen habilitado en su configuración predeterminada a STP, el switch con la dirección MAC más baja será el switch raíz. En la figura 2.14 el switch A es elegido como el switch raíz debido a que tiene la configuración predeterminada de STP y posee la dirección MAC más baja. Sin embargo, debido al tipo de tráfico, capacidad de las interfaces y tipo de conexión, el switch A puede no ser el switch raíz ideal.

Cuando la topología Spanning Tree es calculada en base a los parámetros predeterminados, el camino entre las estaciones fuente y destino puede resultar inadecuado. Por ejemplo, al conectar una interfaz de alta velocidad a otra que tenga un número de revisión mayor que el número del

puerto raíz, es posible ocasionar un cambio del puerto raíz. Este cambio proporcionaría una conexión más rápida hacia el puerto raíz.

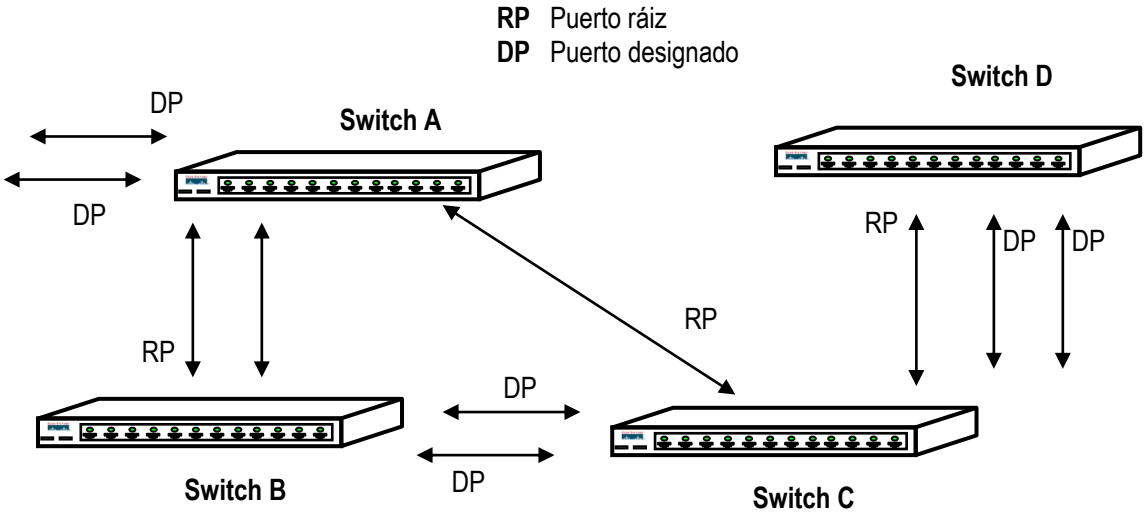


Figura 2.14 Topología Spanning Tree

Supongamos que un puerto en el switch B tiene un enlace con Gigabit Ethernet y que otro puerto en el mismo switch con un enlace 10/100 sea el puerto raíz. El tráfico en la red puede ser más eficiente sobre un enlace con Gigabit Ethernet, al hacer que la prioridad de la interfaz con mayor velocidad sea mayor que la del puerto raíz (valor numérico más bajo), esta interfaz se convertirá en el nuevo puerto raíz.

2.7.3 Conexión de redundancia

Puede crear una conexión principal (backbone) redundante con STP al conectar dos interfaces del switch a otro dispositivo o a dos dispositivos diferentes. Spanning Tree automáticamente deshabilita una interfaz, pero la activa en caso de que la otra interfaz falle, tal como lo muestra la figura 2.15. Si las conexiones son de velocidades distintas, la conexión con menor velocidad estará siempre deshabilitada. Si las velocidades son las mismas, la prioridad para deshabilitar una interfaz dependerá del ID del puerto y

Spanning Tree mantendrá inactiva la conexión que tenga el número más bajo.

2.7.4 Mantenimiento de la conectividad

El tiempo establecido para la duración del direccionamiento dinámico es de 5 minutos, los ajustes se realizan con el comando de configuración global **mac-address-table aging- time**. Sin embargo, la reconfiguración de STP puede ocasionar que muchas estaciones cambien de localización. Por esta causa las estaciones pueden ser inalcanzables, incluso para un tiempo mayor al predeterminado. Durante el proceso de reconfiguración de STP, el tiempo de envejecimiento del direccionamiento puede ser acelerado para que las direcciones de las estaciones puedan salir de la tabla de direccionamiento, y de nueva cuenta ser aprendidas por los switches. La aceleración del tiempo de envejecimiento posee el mismo valor que el parámetro de retraso de reenvió de tramas.

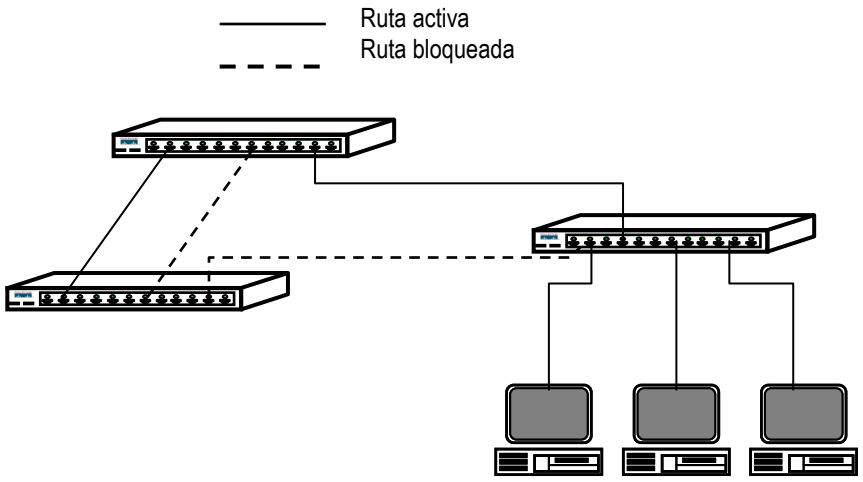


Figura 2.15 Spaning Tree permite configurar una conexión redundante

Por esta razón cada VLAN es tomada como un caso Spanning Tree separado, el switch acelera el tiempo de envejecimiento tomando una base para cada VLAN. Una reconfiguración de STP en una VLAN, ocasionaría que el direccionamiento dinámico aprendido sobre esa VLAN este sujeto al intervalo de envejecimiento ingresado para el switch.

2.7.5 Modos y protocolos STP

Spaning Tree se adapta a las necesidades de cada red, por lo que soporta los siguientes modos y protocolos.

Per VLAN Spanning Tree Plus (PVST+). Este modo esta basado en el estándar IEEE 802.3 y es una extensión propietaria de Cisco. Es el modo utilizado en todas las VLAN basadas en puertos Ethernet, Fast Ethernet y Gigabit Ethernet. PVST+ funciona sobre cada VLAN del switch hasta el máximo soportado, asegurando que cada una tenga una trayectoria libre de loops a través de la red.

PVST+ proporciona equilibrio de carga a nivel capa 2 para la VLAN en la que esté configurado. Puede crear diferentes topologías implementando VLANs para asegurar que todas sus conexiones que estén en uso, no puedan ser suscritas (membership) a otra conexión. Cada caso PVST+ en cada VLAN tiene un único switch raíz, este switch raíz propaga la información Spaning Tree asociada con cada VLAN a todos los demás switches en la red. Por lo tanto, cada switch tiene la misma información de la red y asegura la topología de la red.

Rapid PVST+ Este modo STP opera de manera similar a PVST+, la diferencia radica en el hecho de que esté realiza una convergencia rápida basada en el estándar IEEE 802.1 W (RSTP). Para lograrlo, el Rapid PVST+ elimina inmediatamente el aprendizaje dinámico del direccionamiento MAC

en cuanto recibe un cambio en la topología. En contraste con PVST+, utiliza un tiempo de envejecimiento más corto para el aprendizaje dinámico del direccionamiento MAC, este modo se encuentra disponible si el Enhanced Image se encuentra instalado en el switch.

Múltiple Spanning Tree (MSTP). Esta modalidad de Spanning Tree está basada en el estándar **IEEE 802.1S**. Permite mapear varias VLANs sobre un mismo caso STP, lo cuál reduce el número de STP's requeridos para el soporte de VLANs. MSTP funciona sobre RSTP, el cuál proporciona una rápida convergencia de STP eliminando el retraso de envío para una rápida transición del puerto raíz al estado de reenvío. MSTP no puede funcionar sin RSTP. El uso más común de MSTP es en el backbone y la distribución de una red con conmutación de capa 2.

Preguntas de repaso

1. Defina que es una VLAN.
2. Diga cuales son los tipos de configuración para una VLAN (explique sus diferencias y/o similitudes).
3. Explique cuales son las ventajas que se obtienen al implementar VLAN's.
4. Describa los conceptos de enlace troncal y enlace de acceso.
5. Diga cual es la finalidad del etiquetado de trama.
6. Describa cuales son los métodos de etiquetado de trama existentes.
7. Diga cuales son las operaciones básicas que realizan los dispositivos de conmutación.
8. Explique cual es la diferencia que existe entre la conmutación simétrica y la conmutación asimétrica.
9. Dé la explicación del término "Bufer de Memoria".
10. Diga cuales son los modos de conmutación que utiliza un switch.
11. Explique qué es la conmutación libre de fragmentos.
12. Describa que es una dirección MAC.
13. Explique como es que el switch construye su tabla de direccionamiento MAC.
14. Diga cual es la finalidad del Protocolo de Árbol de Extensión.
15. Dé una explicación de cada uno de los estados del Protocolo de Árbol de Extensión.
16. Diga que es un puerto designado.
17. Diga cuales son los criterios utilizados para seleccionar un switch raíz.

CAPITULO

III

LA INTERFAZ DE LINEA DE COMANDOS

3.1 Introducción al sistema operativo

El Sistema Operativo de Interconexión de Redes (Internetworking Operating System o IOS) de Cisco, es el software que permite al hardware del switch encaminar tramas por una conexión entre redes. Proporciona el conjunto de comandos y funciones de software que permiten controlar y configurar el switch.

Al configurar un switch se debe activar las distintas interfaces que lo integran (Ethernet, FastEthernet, GigabitEthernet), una vez configurado deben gestionarse los archivos de configuración. El conjunto de comandos soportados por el IOS permite llevar a cabo un sin número de tareas, estas tareas pueden resumirse en las siguientes:

1. **Configurar las interfaces LAN**. La configuración de las interfaces LAN debe hacerse después de realizar las conexiones físicas, ensamblar el hardware y conectar los distintos cables a las redes LAN.

2. **Gestionar los archivos de configuración**. Después de realizar la configuración del switch es conveniente guardar una copia de la misma. La configuración de ejecución se almacena en la memoria de acceso no volátil (NVRAM), la cuál se incluye como la configuración de arranque.

3. **Controlar y administrar el switch**. También tendrá que utilizar el conjunto de comandos del IOS para controlar y resolver los posibles problemas que puedan surgir. Por ejemplo, realizar la actualización del IOS.

Para realizar las tareas descritas anteriormente, Cisco proporciona una Interfaz de Línea de Comandos (Command-Line interface o CLI) que puede utilizarse para configurar el switch.

3.2 Estructura de comandos CLI

La interfaz de línea, posee una estructura formada por niveles de acceso llamados modos. Cada modo soporta comandos específicos, sin embargo, existen algunos comandos que permiten realizar acciones de consulta y administración en los distintos niveles de la CLI. Por ejemplo, el comando show, el cuál es una herramienta de análisis comúnmente utilizada en la gestión de redes. La tabla 3.1 describe estos modos soportados por la CLI.

Los comandos de configuración van de lo general a lo específico, primero, se hace saber al IOS que se desea configurar algo, después se le indica ese algo que se desea configurar, y por último, se introducen los parámetros de configuración específicos. Casi toda la configuración del switch sigue este esquema. Existen sin embargo, algunos comandos de configuración que pueden lanzarse en unas pocas líneas, tal es el caso del comando hostname, el cual permite cambiar el nombre al switch. Este comando y otros, son descritos en la sección 3.4 “Funciones Administrativas”. Los comandos de configuración del switch pueden clasificarse en tres categorías:

1. **Comandos Globales**. Son comandos de una sola línea que afectan a toda la configuración del switch. Ejemplo de comandos globales son **hostname** y **enable secret.** Este tipo de comandos se denominan globales porque se aplican a un parámetro que afecta a la funcionalidad general del switch.

Modo	Método de Acceso	Indicador	Salida y acceso al modo siguiente
Usuario	Este es el primer nivel de acceso. Lista la información del sistema, ajustes en las terminales y permite realizar tareas básicas	***Switch>***	Para salir ingrese el comando ***logout***. Para ingresar al modo privilegiado ingrese el comando ***enable.***
Privilegiado	Para entrar a este modo, escriba el comando ***enable.***	***Switch#***	Para regresar al modo usuario ingrese el comando ***disable.*** Para entrar al modo de configuración global ingrese el comando ***configure.***
Configuración Global	En el modo privilegiado, escriba el comando ***configure***.	***Switch(config)#***	Para regresar al modo privilegiado, ingrese el comando **exit** o **end,** o presione **Ctrl-Z**. Para entrar al modo de configuración de interfaz, ingrese el comando ***interface***.
Configuración de Control	En el modo de configuración global, ingrese el comando ***controller longreachethernet.***	***Switch(config-controller)#***	Para regresar al modo de configuración global ingrese ***exit***. Para ir al modo privilegiado ingrese ***Ctrl-Z o End***.
Configuración de Interfaz	Estando en el modo global ingrese el comando ***interface*** (especificando la interfaz)	***Switch(config-if)#***	Para ir al modo global ingrese ***exit.*** Para ir al modo privilegiado ingrese *Ctrl-Z o End*.
Configuración de Secuencia	En el modo de configuración global especifique la secuencia mediante el comando ***lre sequence***.	***Switch(config-seq)#***	Para salir al modo de configuración global ingrese ***exit***. Utilice el comando ***Ctrl-Z o end*** para regresar al modo privilegiado.
Config-vlan	En modo global ingrese el comando ***vlan*** *vlan-id*	***Switch(config-vlan)#***	Para salir al modo de configuración global ingrese ***exit*** Para regresar al modo privilegiado presione ***Crtl-Z***.
Configuración VLAN	En el modo privilegiado ingrese el comando ***vlan database.***	***Switch (vlan)#***	Para salir al modo de configuración global ingrese ***exit***

Tabla 3.1 Modos de comandos soportados por el IOS del switch

2. **Comandos de puerto**. Son un conjunto de comandos que permiten especificar o controlar la configuración de alguna interfaz. A estos comandos deben seguirles una serie de subcomandos, los cuales proporcionan la información adicional de configuración de la interfaz. Por ejemplo, el comando **interface fastethernet0/2** permite indicarle al switch que debe configurar la interfaz FastEthernet 2 a determinada VLAN.

3. **Subcomandos**. Los subcomandos proporcionan la información específica de configuración de la interfaz, la cual ha sido especificada mediante un comando de puerto. Por ejemplo, asignar una dirección IP al switch para realizar la conexión vía Telnel.

3.2.1 Modo usuario EXEC

El IOS de Cisco utiliza un intérprete para ejecutar los comandos (interpreta el comando y después lo ejecuta) denominado Exec. El modo Usuario y Privilegiado se consideran niveles distintos del intérprete Exec. Por ello, cuando se lanza alguno de estos modos, los comandos allí disponibles revisten una determinada estructura básica (descrita en la sección 3.4 “Funciones Administrativas”).

Después de acceder al dispositivo, este se iniciará automáticamente en el modo Usuario. Los comandos disponibles en el nivel de usuario están incluidos en el modo Privilegiado. En general, los comandos proporcionados en este nivel, se usan para realizar cambios temporales en alguna interfaz, realizar pruebas básicas y listar la información del sistema.

Los comandos soportados pueden variar dependiendo de la versión del IOS que se utilice. Para ver una lista detallada de los comandos, ingrese el símbolo de interrogación en el indicador del modo usuario.

3.2.2 Modo Privilegiado EXEC

Debido a que los comandos de este modo permiten ajustar los parámetros de operación del switch, el acceso debe ser protegido por contraseña, de esta manera, algún usuario no autorizado no tendrá opción para modificar la configuración. El modo privilegiado incluye los comandos del modo usuario. Si el administrador de sistemas ajustó alguna contraseña, debe ser ingresada en el indicador del modo usuario para conceder el acceso al modo privilegiado. Por cuestiones de seguridad, la contraseña es cifrada, por lo que no aparecerá en la pantalla, además de ser sensible a mayúsculas y minúsculas.

Los comandos soportados pueden variar dependiendo de la versión del IOS que se utilice. Para ver una lista detallada de los comandos disponibles, ingrese el símbolo de interrogación en el indicador del modo en el que se encuentre. En la sección 3.3 “Sistema de ayuda del IOS” se ofrece una descripción detallada de las distintas formas de obtener ayuda.

3.2.3 Modo de Configuración Global.

Los comandos del modo de configuración global se aplican a las características que afectan a todo el dispositivo. Use el comando ***configure*** en el modo privilegiado para entrar al modo de configuración. Por defecto, estos comandos se ingresan en la consola de administración.

Cuando ingresa el comando ***configure***, aparecerá en la pantalla un mensaje que indica la fuente de configuración de comandos.

Switch# **configure**
Configuring from terminal, memory, or network [terminal]?

Los comandos soportados pueden variar dependiendo de la versión del IOS que se utilice. Para ver una lista detallada de los comandos disponibles ingrese el símbolo de interrogación en el indicador del modo.

3.2.4 Modo Configuración de Control

Los comandos de este modo se utilizan para realizar actualizaciones de firmware en LRE Switches (Long Reach Ethernet), pero raramente es usado.

Los comandos del modo de configuración de control se encuentran en un nivel superior a los comandos del modo global. Use el comando ***controller longreachethernet*** *interface-id* para acceder al modo de control.

3.2.5 Modo de Configuración de Interfaz

Modifica la operación de la interfaz, los comandos disponibles en este modo siempre siguen a los del modo de configuración global.

Use el comando ***interface*** *type_ number.subif* para acceder al modo de configuración de la interfaz. Los comandos soportados pueden variar dependiendo de la versión del IOS que se utilice. Para ver una lista detallada de los comandos disponibles ingrese el símbolo de interrogación en el indicador del modo.

3.2.6 Modo de configuración de Secuencia

Los comandos de configuración de secuencia se aplican solo a las interfaces Long Reach Ethernet (LRE). Use este comando para crear una secuencia o añadir perfiles a una secuencia existente. Utilice el comando **Ire sequence** *sequence-name* para ingresar a este modo de configuración. El indicador del modo de configuración de secuencia deberá se el siguiente:

Switch (config-seq) #

Para salir al modo de configuración global ingrese ***exit***. Utilice el comando ***Ctrl-Z o end*** para regresar al modo privilegiado.

3.2.7 Modos VLAN

Existen dos modos para configurar VLANs, la elección del modo de configuración depende del tipo de VLANs que se va a establecer, en el capítulo cuatro se describen las opciones de configuración y las consideraciones que debe de tomar cuando seleccione cada método. Estos modos son los siguientes:

1. ***Modo config-vlan.*** Use este método para configurar VLANs en el rango normal (VLAN ID de 1 a 1005) cuando VTP se encuentre en el modo transparente ó para configurar VLANs en el rango extendido (VLAN ID de 1006 a 4094) cuando el Enhanced Software Image esté instalado. Cuando VTP esta en modo transparente, la configuración VLAN es almacenada en el archivo running configuration**,** si VTP se encuentra en el modo transparente o servidor, las VLANs configuradas en el rango normal serán almacenadas en la base de datos VLAN. Las VLAN configuradas en el rango extendido no son almacenadas en la base de datos. VTP es escrito con mayor detalle en el anexo C.

2. ***Modo VLAN Configuración.*** Puede usar este modo para crear o modificar los parámetros de VLANs configuradas en rango normal. En el modo privilegiado, escriba el comando ***vlan database*** y pulse Enter para acceder al modo de configuración VLAN.

Estos modos de configuración se describen con mayor detalle en el capítulo 4, “Configuración de VLANs”.

3.2.8 Modo de Configuración de Línea

Los comandos de este modo modifican la operación del terminal de línea. Use estos comandos para realizar ajustes de los parámetros, línea por línea o para un rango de líneas.

Use el comando **line vty** *line_number* [*ending_line_number*] para ingresar al modo de configuración de línea. Este comando y otros, son utilizados en la sección 3.4 “Funciones Administrativas”, donde se realiza la configuración de sus respectivos parámetros.

3.3 El sistema de ayuda del IOS

Al margen del modo en el que se encuentre, el IOS puede proporcionar ayuda. El sistema de ayuda se encuentra disponible en los modos Usuario, Privilegiado y Configuración. Si se encuentra en el modo usuario, y desea ver un listado completo de los comandos disponibles, solo tiene que introducir **?** y después pulsar Enter. El listado de comandos aparecerá en la pantalla de la consola como se muestra en la figura 3.1.

Una vez consultados los comandos disponibles en el modo usuario, decide utilizar un determinado comando, pero no sabe exactamente como debe introducirse en el indicador. Por ejemplo, quiere saber como se utiliza el comando show. Para ello, tiene que escribir show (o el comando del que desee obtener ayuda) en el indicador seguido del signo **?**, y después pulsar Enter, el sistema le proporcionará la ayuda especifica para el comando

seleccionado (en el caso de estar soportado por el IOS), tal y como se muestra en la figura 3.2.

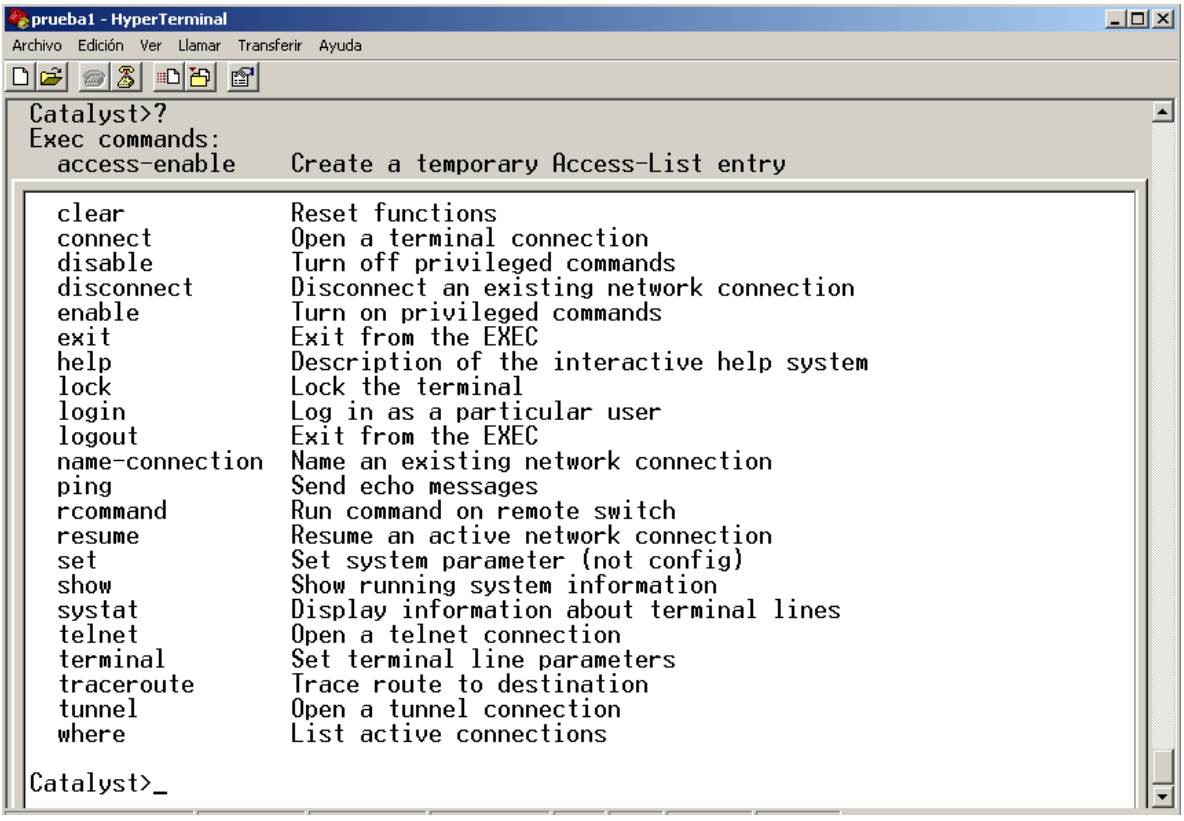

prueba1 - HyperTerminal
Archivo Edición Ver Llamar Transferir Ayuda
Catalyst>?
Exec commands:
access-enable Create a temporary Access-List entry
clear Reset functions
connect Open a terminal connection
disable Turn off privileged commands
disconnect Disconnect an existing network connection
enable Turn on privileged commands
exit Exit from the EXEC
help Description of the interactive help system
lock Lock the terminal
login Log in as a particular user
logout Exit from the EXEC
name-connection Name an existing network connection
ping Send echo messages
rcommand Run command on remote switch
resume Resume an active network connection
set Set system parameter (not config)
show Show running system information
systat Display information about terminal lines
telnet Open a telnet connection
terminal Set terminal line parameters
traceroute Trace route to destination
tunnel Open a tunnel connection
where List active connections
Catalyst>_

Figura 3.1 Lista de comandos disponibles en el modo Usuario

Como se mencionó anteriormente, el sistema de ayuda también está disponible en los modos Privilegiado y Configuración. La ayuda del modo privilegiado se parece a la suministrada en el modo usuario. Para obtener información general, introduzca el carácter de interrogación, si desea información más específica, solo escriba el comando seguido de dicho carácter.

Cuando la información de ayuda (que ofrece determinado comando como ?) no cabe en la pantalla de la consola, aparecerá la palabra More al final de la información mostrada. Para ver el resto de la información, deberá pulsar

Enter para avanzar una línea y pulsar la barra espaciadora para ir a la pantalla siguiente. Si no quiere ver más información y desea volver al indicador de la consola pulse la tecla Esc.

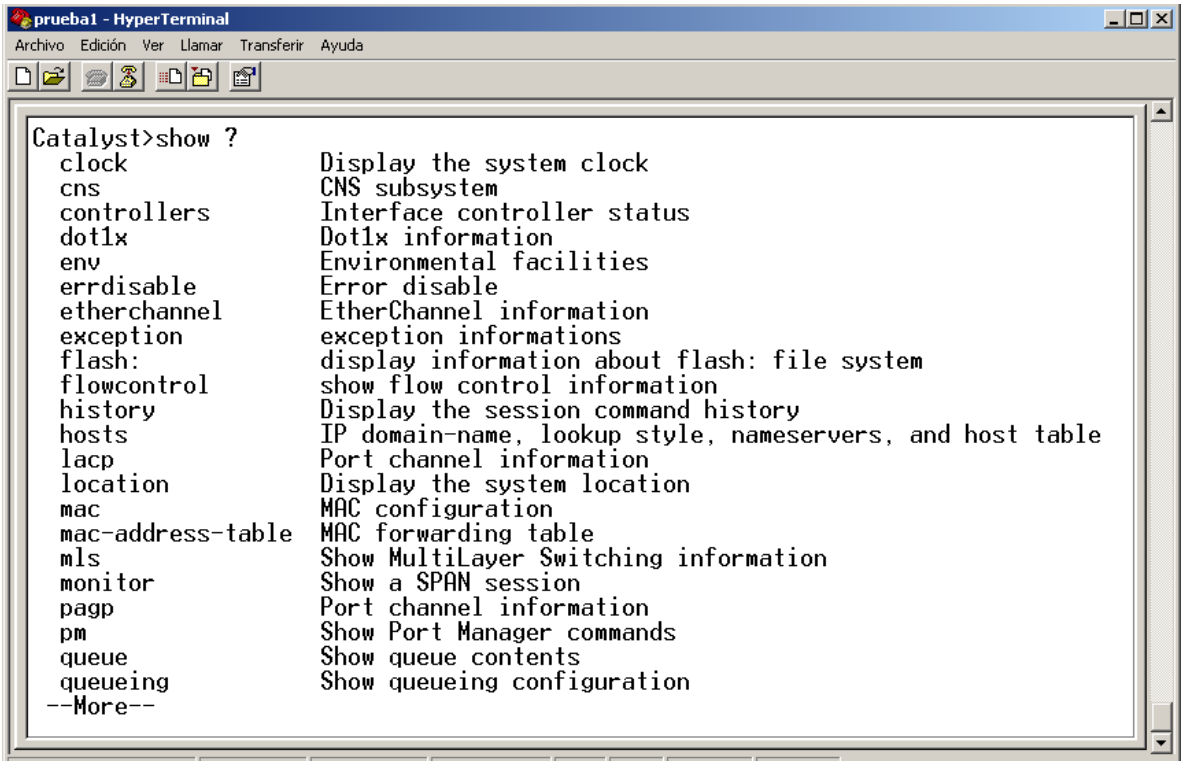

prueba1 - HyperTerminal
Archivo Edición Ver Llamar Transferir Ayuda
Catalyst>show ?
clock Display the system clock
cns CNS subsystem
controllers Interface controller status
dot1x Dot1x information
env Environmental facilities
errdisable Error disable
etherchannel EtherChannel information
exception exception informations
flash: display information about flash: file system
flowcontrol show flow control information
history Display the session command history
hosts IP domain-name, lookup style, nameservers, and host table
lacp Port channel information
location Display the system location
mac MAC configuration
mac-address-table MAC forwarding table
mls Show MultiLayer Switching information
monitor Show a SPAN session
pagp Port channel information
pm Show Port Manager commands
queue Show queue contents
queueing Show queueing configuration
--More--

Figura 3.2 Puede obtener ayuda sobre algún comando en particular

En la figura 3.3 se muestra la pantalla de ayuda para el modo privilegiado. Como puede observar, proporciona un mayor número de comandos que el modo usuario, razón por la cual, este modo se encuentra protegido por contraseña.

El sistema operativo del switch, proporciona varias opciones de ayuda para las entradas en la línea de comandos, las cuales son:

1. **Ayuda relativa al contexto**. Proporciona una lista de los argumentos asociados con cada comando específico.

2. **Mensajes de error de consola**. Identifica los problemas relacionados con los comandos que han sido introducidos incorrectamente.
3. **Búfer de historial de comandos**. Permite volver a llamar largos y complicados comandos o entradas para volver a ejecutarlos, revisarlos o corregirlos.

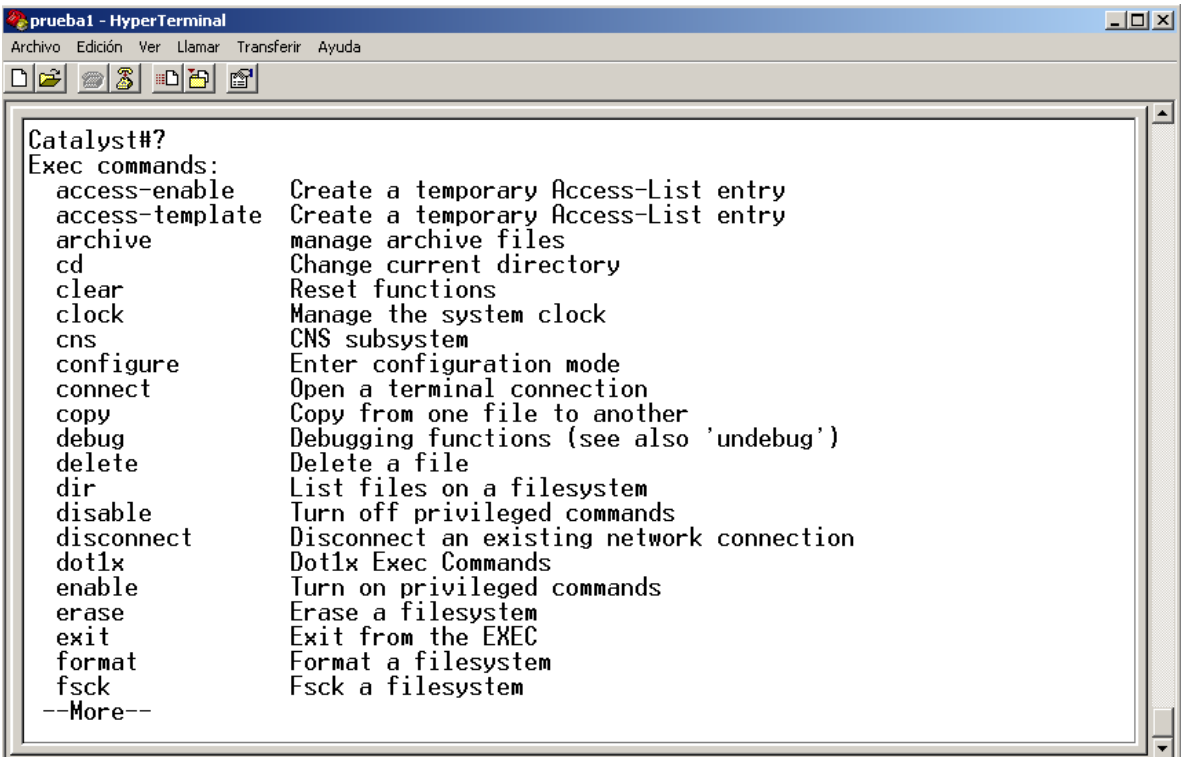

prueba1 - HyperTerminal
Archivo Edición Ver Llamar Transferir Ayuda
Catalyst#?
Exec commands:
access-enable Create a temporary Access-List entry
access-template Create a temporary Access-List entry
archive manage archive files
cd Change current directory
clear Reset functions
clock Manage the system clock
cns CNS subsystem
configure Enter configuration mode
connect Open a terminal connection
copy Copy from one file to another
debug Debugging functions (see also 'undebug')
delete Delete a file
dir List files on a filesystem
disable Turn off privileged commands
disconnect Disconnect an existing network connection
dot1x Dot1x Exec Commands
enable Turn on privileged commands
erase Erase a filesystem
exit Exit from the EXEC
format Format a filesystem
fsck Fsck a filesystem
--More--

Figura 3.3 El modo Privilegiado dispone de una cantidad mayor de comandos

3.3.1 Ayuda relativa al contexto.

Un signo de interrogación durante una sesión EXEC proporciona siempre ayuda en pantalla. Se dispone de dos tipos de ayuda relativa al contexto; ***ayuda de texto y ayuda relativa a la sintaxis de un comando***. Como se

muestra en la figura 3.1, puede utilizar **?** para obtener una lista de todos los comandos que comienzan por una secuencia de caracteres determinada. Para ello, escriba el carácter o caracteres seguidos del signo "?". No incluya ningún espacio de separación delante del signo de interrogación, la consola mostrará una lista de todos los comandos que comienzan con los caracteres especificados.

También puede usar el signo de interrogación para conseguir ayuda acerca de la sintaxis específica de un comando. Al introducir este carácter, en lugar de una palabra clave o argumento cuya sintaxis no está segura, IOS mostrará una lista de las operaciones disponibles para el comando en cuestión.

3.3.2 Mensajes de error de consola.

Los mensajes de error que aparecen con mayor frecuencia en la consola se muestran en la figura 3.4. Estos mensajes en realidad son un sistema de ayuda, que permite identificar los problemas relacionados con entradas de comandos incorrectas. El mensaje le ayudará a averiguar cómo debe modificar el comando en la línea y corregir el problema. La tabla 3.5 muestra un listado que describe algunos errores CLI comunes y explica cómo obtener ayuda para resolverlo.

3.3.3 Historial de comandos

Revisar el historial de comandos proporciona una lista del contenido del búfer de sustitución del switch. Se trata de una lista de los comandos introducidos recientemente. Para ver dichos comandos, introduzca ***history***, el resultado se muestra en la figura 3.5.

A continuación verá una lista de los comandos utilizados recientemente, esto le permitirá volver a utilizar cualquiera de ellos, sin necesidad de teclearlo de nuevo. Para aplicar nuevamente un comando introducido con anterioridad, pulse la tecla flecha arriba. Al seguir pulsando esa misma tecla, accederá a otros comandos anteriores. Algunos teclados no disponen de tecla flecha arriba, o es posible que la aplicación no soporte el uso de dichas teclas. Una alternativa a la flecha arriba, es la combinación de teclas ctrl+p.

Mensajes de Error	Significado	Como obtener ayuda
%Ambiguous Command: "show con"	No se han introducido suficientes caracteres para que el switch pueda reconocer la orden.	Vuelva a introducir la orden seguida de un signo de interrogación sin espacio entre la instrucción y dicho signo.
%Incomplete command	No se han introducido todas las palabras clave o valores requeridos por la orden.	Vuelva a introducir la orden seguida de un signo de interrogación con un espacio entre el comando y el signo.
% Invalid input Detected at ´^´ marker	Se ha introducido la orden incorrectamente. El símbolo marca el punto donde se ha detectado el error.	Introduzca un signo de interrogación para obtener un listado de todos los comandos que estén disponibles en este modo.

Tabla 3.5 Mensajes de error CLI comunes

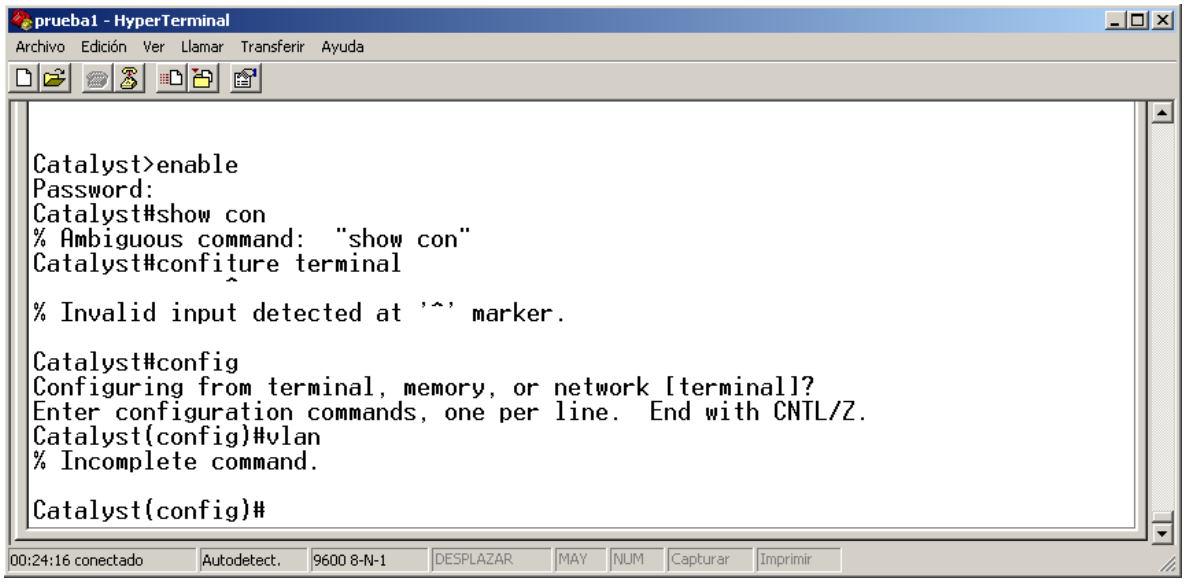


Figura 3.4 Los mensajes de error resultan una fuente de ayuda.

Para recorrer el historial de comandos en sentido inverso, puede usar la combinación de teclas ctrl+n. Una vez que llegue al comienzo o el final de la lista, seguirán mostrándose más comandos. La tabla 3.6 describe las combinaciones de teclas utilizadas en el historial de comandos.

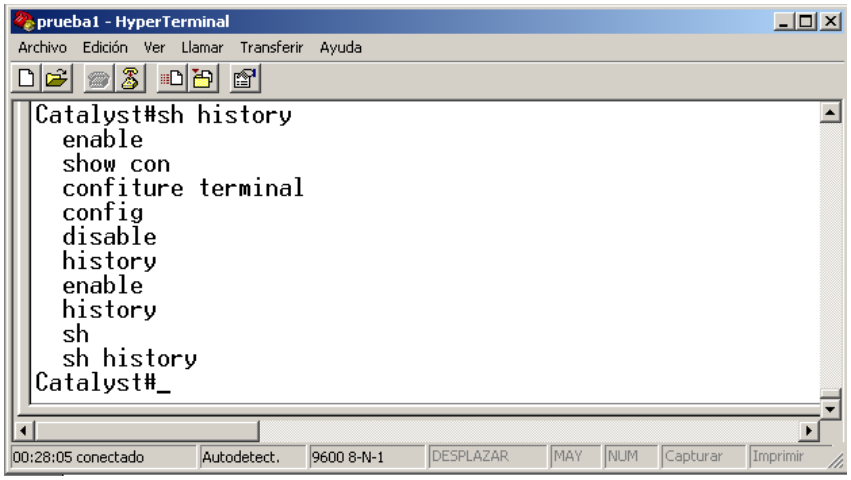


Figura 3.5 Es posible ejecutar nuevamente algún comando introducido con anterioridad

Combinación de teclas	Funcionalidad
Ctrl+p o tecla flecha arriba	Permite desplazarse en la CLI para consultar ó utilizar algún comando introducido al inicio de la configuración.
Ctrl+n tecla ficha abajo	Permite desplazarse en la CLI para consultar ó utilizar algún comando introducido al final de la configuración.
Switch>show history	Muestra el contenido del búfer de comandos.

Tabla 3.6 Desplazamiento en el historial de comandos

3.4 Funciones Administrativas

Las cuestiones administrativas son muy importantes para el control de la red, principalmente las que se refieren a la seguridad de los equipos. Cada IOS soporta determinados comandos que ayudan a la administración de la red, tales comandos, proporcionan funciones administrativas que puede configurar en un switch.

Las funciones administrativas que puede configurar en un switch son las siguientes:

1. Nombre del equipo (hostname)
2. Mensajes (Banners)
3. Contraseñas (password)
4. Descripción de las interfaces

Cabe señalar, que estas funciones no hacen que su equipo sea mejor o más rápido, pero por cuestiones de seguridad es recomendable que configure estas opciones en el switch y (en el caso de soportarlas) en todos los demás dispositivos de la red.

Es importante señalar, que estas funciones administrativas se implementan en un switch o router Cisco empleando los mismos comandos. Aunque estas funciones pueden variar dependiendo del modelo y la versión del IOS que se este ejecutando.

3.4.1 Nombre del equipo

Una red puede estar compuesta por una gran cantidad de switchs interconectados, el comando ***hostname*** permite identificar mediante un nombre cada switch. Esta manera de identificación solo tiene un significado local, ya que no se difunde a través de la red, sin embargo, puede utilizarse para propósitos de autentificación. La figura 3.6 muestra como se realiza la configuración del nombre del switch. Para realizarla, lleve a cabo los pasos siguientes:

1. Ingrese al modo Privilegiado, si ha establecido una contraseña secreta para este modo, deberá ingresarla, recuerde que ésta se encuentra cifrada, por lo que no aparecerá en la pantalla de la consola.
2. Para lanzar el modo de configuración, escriba el comando **configure terminal**, el indicador se muestra en la figura 3.6.
3. Escriba el comando **hostname**, seguido del nombre del switch y a continuación pulse Intro. Como podrá observar, el nombre seleccionado es Catalyst-A.
4. No olvide salir de los modos de configuración y privilegiado.

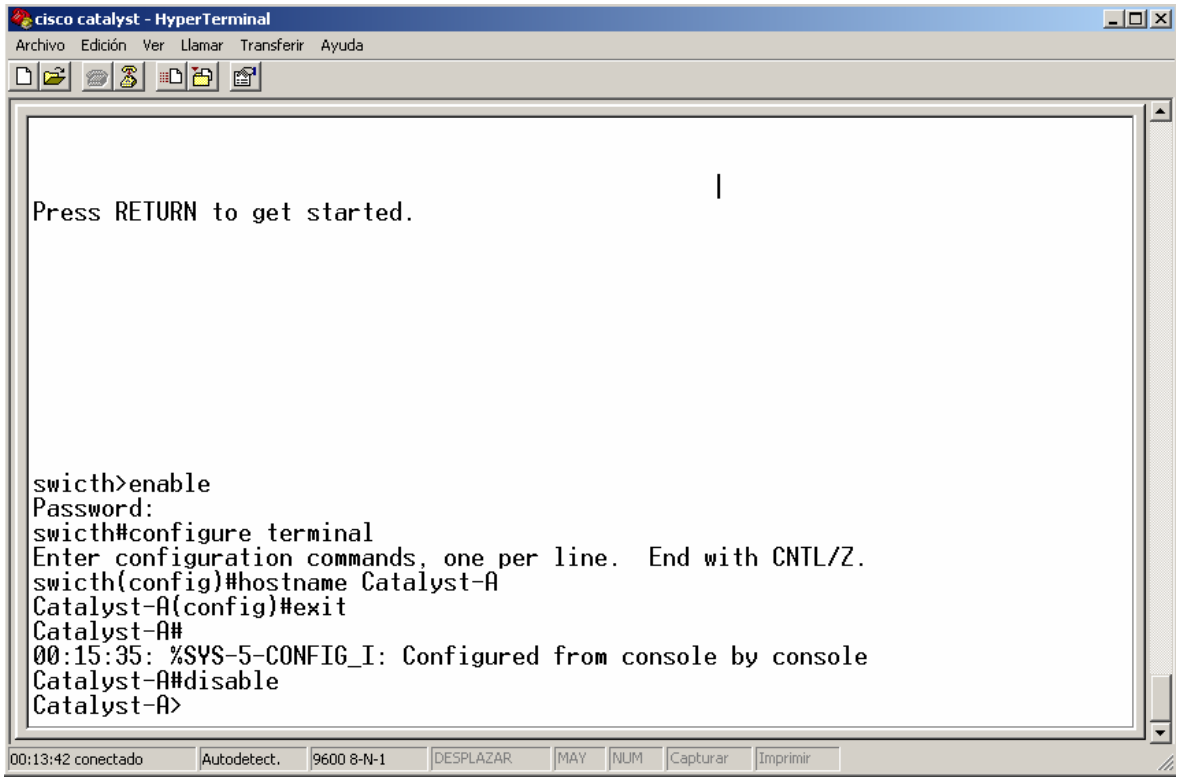


Figura 3.6 Configuración del nombre del switch

3.4.2 Mensajes

Una de las razones para crear un banner, es dar un aviso de seguridad a todo aquel que intente ingresar al switch, ya sea por el puerto de consola o a través de una sesión Telnet.

Como se muestra en la figura 3.7, es posible implementar seis tipos de mensajes, los más utilizados son: mensajes para el modo Exec (Exec banner), mensajes de terminal de línea (Incoming banner), registros (login banner) y mensajes del día (portadas). El mensaje del día (MODT) es el banner más utilizado, éste proporciona un mensaje a toda persona que

pretenda conectarse al switch vía telnet, por algún puerto auxiliar o a través del puerto de consola.

Al crear una portada para el switch, debe seleccionar un carácter que no vaya a ser empleado en la estructura de la portada. Como por ejemplo, el símbolo $ o algún otro.

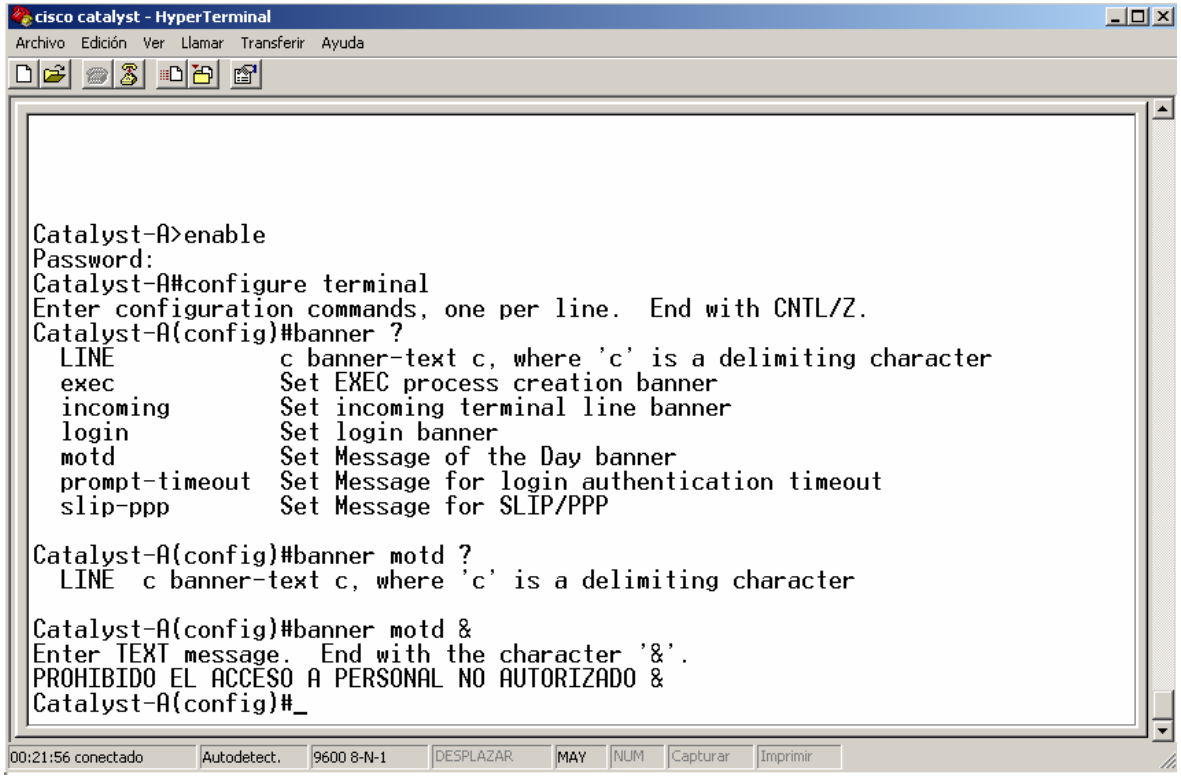

cisco catalyst - HyperTerminal
Archivo Edición Ver Llamar Transferir Ayuda
Catalyst-A>enable
Password:
Catalyst-A#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Catalyst-A(config)#banner ?
LINE c banner-text c, where 'c' is a delimiting character
exec Set EXEC process creation banner
incoming Set incoming terminal line banner
login Set login banner
motd Set Message of the Day banner
prompt-timeout Set Message for login authentication timeout
slip-ppp Set Message for SLIP/PPP
Catalyst-A(config)#banner motd ?
LINE c banner-text c, where 'c' is a delimiting character
Catalyst-A(config)#banner motd &
Enter TEXT message. End with the character '&'.
PROHIBIDO EL ACCESO A PERSONAL NO AUTORIZADO &
Catalyst-A(config)#_
00:21:56 conectado
Autodetect.
9600 8-N-1
DESPLAZAR
MAY
NUM
Capturar
Imprimir

Figura 3.7 Configuración de un aviso de seguridad.

Para crear una portada en el switch, realice lo siguiente:

1. Ingrese al modo de configuración, ya que es en éste, donde se crea la portada del switch.
2. Escriba el comando **banner mod** [*carácter*], donde *carácter* corresponde a un carácter de teclado elegido por el usuario, el cual marca el final del texto escrito en la portada.
3. Salga del modo de configuración.

Tras salir del modo Configuración, es posible que tenga que volver a pulsar una vez más Enter para situarse en el indicador del modo privilegiado. Para ver la portada debe introducir el comando ***quit*** y después pulsar Enter. Si ha establecido una contraseña para el switch, el sistema le pedirá que la introduzca para reiniciar la sesión.

Como podrá observar en la figura 3.7, existen seis tipos de mensajes que puede ajustar en la consola, sin embargo, no todos suelen ser utilizados, por lo que solo se describen los principales.

1. **EXEC banner.** Permite crear un banner de línea de activación que aparecerá cuando se inicie un proceso Exec (como una conexión mediante el terminal virtual) o al comienzo de alguna sesión a través del puerto de consola.

2. **Incoming banner**. Puede utilizar esta opción para desplegar un mensaje sobre las terminales conectadas o para sesiones Telnet reservadas. Éste tipo es muy útil para proporcionar instrucciones a nuevos usuarios.

3. **Login banner.** Este tipo de mensaje puede configurarse para ser mostrado en todas las terminales activas y aparecerá después del mensaje MOTD. Este modo puede ser deshabilitado sobre alguna interfaz o deshabilitarse globalmente con el uso del comando ***no banner login.***

3.4.3 Ajuste de contraseñas

Existen diversos tipos de contraseñas que pueden implementarse en el switch cisco: consola, auxiliar, Telnet (VTY), contraseña secreta y contraseña de activación. Las dos últimas se utilizan para ajustar una contraseña que

proteja el acceso al modo privilegiado. Las restantes son usadas para configurar una contraseña que proteja el acceso al modo usuario a través del puerto de consola, el puerto auxiliar o vía Telnet. Estas contraseñas pueden variar dependiendo del modelo del equipo en el que sean ajustadas, para el caso del switch 2950, las opciones disponibles se observan en la figura 3.8.

3.4.3.1 Enable secret y enable password

Los parámetros que conforman la contraseña de activación son los siguientes:

- **Leas-resort**. Permite ingresar al switch si la autentificación es a través de un servidor TACACS y este no se encuentra disponible.
- **Password.** Habilita la contraseña de activación que era utilizada en versiones del IOS anteriores, y regularmente no se usa si se ha ajustado la contraseña secreta.
- **Secret.** Este parámetro permite cifrar la contraseña y al estar activo anula la contraseña de activación.
- **Use-tacacs.** Permite realizar la autentificación a través de un servidor TACACS. Esto es conveniente si tiene varios switch en la red y desea cambiar la contraseña en cada equipo. El servidor reduce la tarea de configurar cada equipo y permite hacer el ajuste una sola vez.
- **Aux y Console** Ajustan las contraseñas para el puerto auxiliar y de consola.

Por cuestiones de seguridad, el IOS no permite que la contraseña para el modo secreto y de activación sean las mismas. Si por alguna razón, estas contraseñas coinciden, el sistema arrojará un mensaje de error.

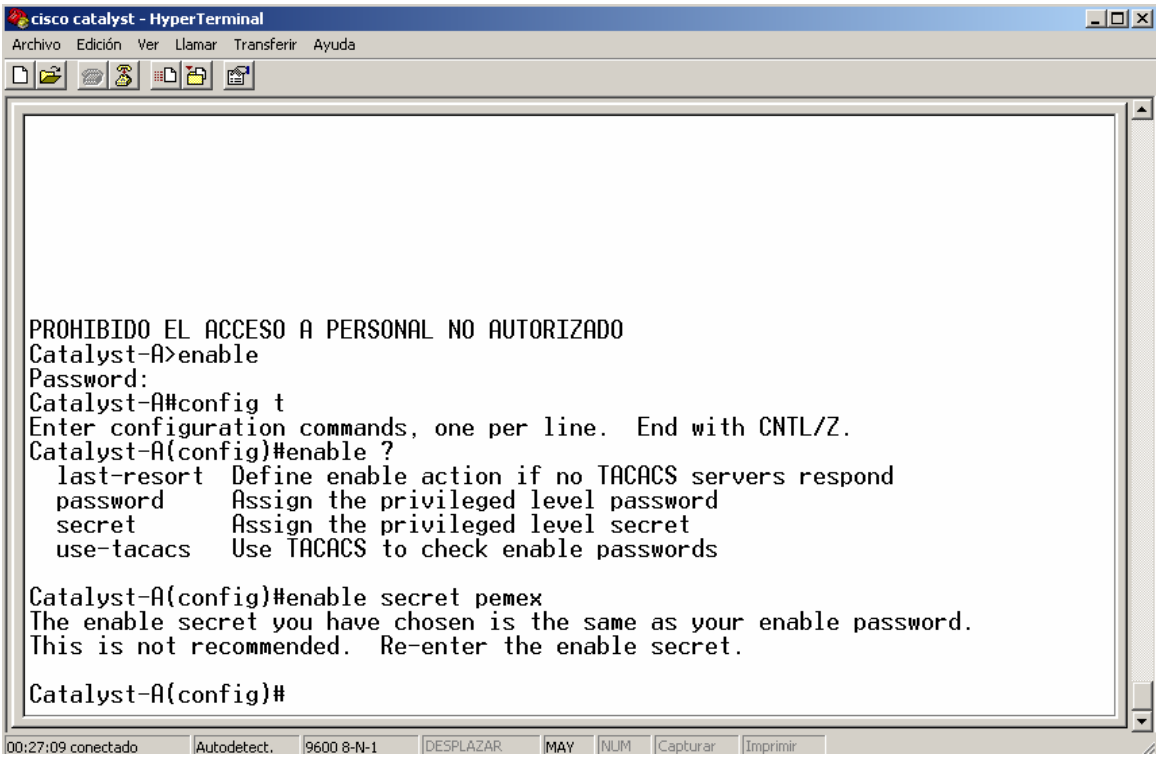

cisco catalyst - HyperTerminal
Archivo Edición Ver Llamar Transferir Ayuda
PROHIBIDO EL ACCESO A PERSONAL NO AUTORIZADO
Catalyst-A>enable
Password:
Catalyst-A#config t
Enter configuration commands, one per line. End with CNTL/Z.
Catalyst-A(config)#enable ?
last-resort Define enable action if no TACACS servers respond
password Assign the privileged level password
secret Assign the privileged level secret
use-tacacs Use TACACS to check enable passwords
Catalyst-A(config)#enable secret pemex
The enable secret you have chosen is the same as your enable password.
This is not recommended. Re-enter the enable secret.
Catalyst-A(config)#
00:27:09 conectado
Autodetect.
9600 8-N-1
DESPLAZAR
MAY
NUM
Capturar
Imprimir

Figura 3.8 Contraseñas disponibles en el switch

3.4.3.2 Console Passwords

En el modo de configuración, ingrese el comando ***line console ?***. Observará que dispone de la opción cero debido a que solo cuenta con un puerto. En el caso de contar con más puertos, puede configurarlos con la misma contraseña, pero por razones de seguridad no se recomienda.

Existe otro comando que es muy utilizado para las conexiones por el puerto de consola, este es el comando ***Exec-timeout,*** el cual permite ajustar el tiempo de respuesta para una sesión en la consola. El tiempo de respuesta predeterminado es de 10 minutos. Para evitar problemas ajuste el tiempo a cero (exec-timeout 0 0), con lo cuál el tiempo nunca se agotara y su conexión permanecerá activa.

3.4.3.3 Telnet Passwords

Este comando permite ajustar una contraseña para el acceso al switch a través de la consola, para hacerlo use el comando ***line vty*** . Los switchs que no cuenten con la edisión Enterprise del Cisco IOS tienen por defecto cinco lineas vty (de 0 hasta 4), la figura 3.9 muestra que al ingresar el comando ***line vty 0*** el sistema mostrará el número de líneas que proporciona la edición que se ejecuta en el switch.

Si desea conectarse al switch sin tener que ingresar una contraseña puede utilizar el comando ***no login*** para desactivar esta opción.

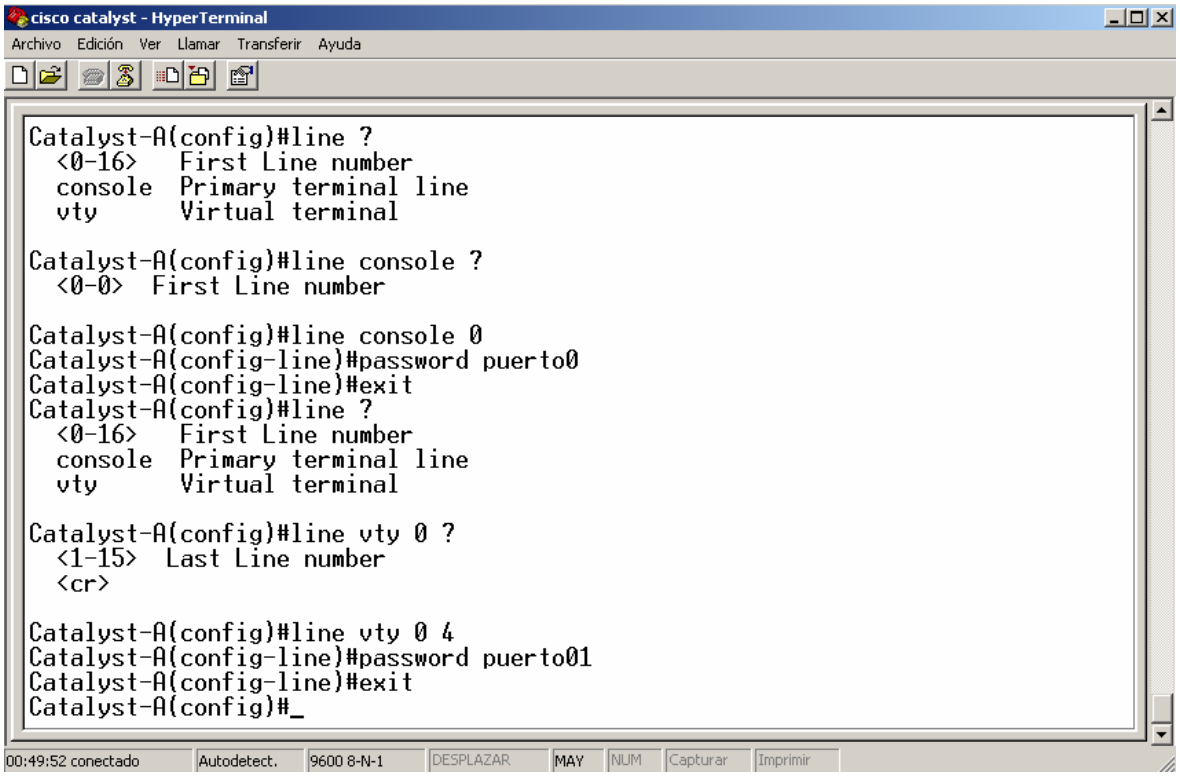


Figura 3.9 Configuración de la contraseña de consola y de términal virtual

Preguntas de repaso

18. Explique cuales son las tareas que pueden realizarse mediante la línea de comandos soportada en el switch.
19. Diga cuales son los modos de comandos soportados por el switch.
20. Diga cual es la clasificación general de los comandos de configuración soportados en el switch.
21. Explique cual es la diferencia de los tres modos de comandos en la interfaz de línea de comandos.
22. Describa los modos de configuración de una VLAN.
23. Explique la diferencia al solicitar ayuda en los distintos modos de comandos soportados por el IOS.
24. Diga cuales son las opciones de ayuda proporcionadas por el sistema operativo del switch.
25. Diga cuales son los tipos de ayuda relativa al contexto.
26. Describa cuales son las funciones administrativas que pueden implementarse en el switch.
27. Describa los tipos de contraseñas que pueden configurarse en un switch.

CAPITULO

IV

CONFIGURACION DE REDES DE AREA LOCAL VIRTUALES

4.1 Soporte de VLANs

Los switchs que funcionan con la versión estándar del Software Image (SI) soportan 64 VLANs, los switches catalyst 2950 que funcionan con la versión Enhanced Image Software (EI) soportan 250 VLANs. Estas VLANs se identifican mediante un número que va de 1 a 4094 cuando el EI esta instalado, y de 1 a 1005 para el caso del SI. Los IDs de 1002 a 1005 están reservados para identificar VLANs en redes Token Ring y FDDI.

VTP solo reconoce VLANs en el rango normal, los identificadores mayores a 1005 se encuentran reservados para la configuración de VLANs en el rango extendido y no son almacenados en la base de datos de VLANs. Si desea crear VLANs en el rango extendido es necesario ajustar VTP al modo transparente.

4.2 Modos de asignación de puertos

Puede configurar un puerto para que pertenezca a una VLAN mediante algún tipo de membresía, está determinará el tráfico que dicho puerto pueda trasportar, así como también el identificador de VLAN designado en el switch.

Los modos de membresía y sus características VTP descritas en cada modo se describen a continuación.

1. **Static-access**. En este tipo de puertos la asignación a una VLAN se hace manualmente. Este modo no requiere de los servicios proporcionados por VTP. Si no es necesario que la información que procesa este protocolo sea difundida por la red, entonces, deberá ajustar VTP al modo transparente. Para que VTP participe en el intercambio de avisos, debe configurar un puerto del switch como un

enlace troncal y conectarlo a otro puerto igualmente configurado en otro switch.

2. **802.1Q** .Por defecto, un puerto de enlace troncal será miembro de todas la VLANs, incluyendo las del rango extendido. Sin embargo, la membresía puede limitarse al configurar una lista de VLANs permitidas en algún puerto. También puede modificar la lista de reducción (pruning-elegible list) para bloquear el flujo de tramas, y evitar que estas viajen hacia otros puertos troncales. En este modo de membresía no se requiere el uso de VTP, sin embargo, es recomendable utilizarlo debido a que mantiene una configuración coherente de las VLANs y facilita el control de la adicción, depuración o renombre de VLANs en la red. VTP intercambia mensajes de configuración de VLAN sobre enlaces troncales.

3. **Dynamic access**. La membresía para configurar un puerto con acceso dinámico está reservada para VLANs configuradas en el rango normal y es asignada en forma dinámica por un VLAN Management Policy Server (VMPS). El VMPS puede ser un switch Catalyst 5000 o 6000, pero nunca un Catalyst 2950 o 2955. Puede configurar puertos de acceso dinámico y troncal en el mismo switch, pero debe de conectar los puertos de acceso dinámico a una estación final y no a otro switch. Este modo de membresía requiere que VTP este habilitado en el switch.

4. **Voice VLAN**. Un puerto que trasporte voz en una VLAN, es un puerto de acceso al cual se conectará un teléfono IP (de Cisco o algún otro fabricante). Si un puerto es configurado para el trasporte de voz, no requerirá de los servicios de VTP, ya que éste no interviene en el tráfico de voz.

4.3 Configuración de VLANs en el rango Normal

Las VLANs en el rango normal son aquellas que poseen un identificador en el rango de 1 a 1005. Si VTP se configura en modo servidor o transparente, será posible añadir, modificar o eliminar las VLANs del archivo vlan.dat (las VLAN 2, 1002 a 1005 son creadas automáticamente y no pueden ser removidas).

Las configuraciones de VLANs en el rango normal son escritas en el archivo *vlan.dat* (VLAN database), este archivo es guardado en la NVRAM y puede ser consultado ingresando el comando ***show vlan*** en el modo privilegiado.

Para definir el tipo de membresía asociado a un puerto, añadir, modificar o eliminar la configuración VLAN. Puede utilizar los comandos disponibles en el modo de configuración de interfaz. Los resultados de estos comandos son escritos en el archivo de configuración y pueden consultarse con el comando show ***running-config*****.**

Cuando crea una VLAN en el rango normal o modifica una existente, los parámetros que puede ajustar son los siguientes:

1. Identificador de VLAN
2. Nombre de la VLAN
3. Tipo de VLAN (Ethernet, Token Ring, FDDI, Token Ring Net, etc.)
4. Estado de la VLAN (activo o suspendido)
5. Unidad máxima de transmisión (MTU)
6. Identificador de seguridad
7. Número de anillo para FDDI
8. Ajuste del Protocolo Spaning Tree
9. Número de VLAN utilizado para el cambio de VLAN

4.3.1 Consideraciones generales

Antes de configurar o modificar una VLAN en el rango normal, debe tomar en cuenta las consideraciones siguientes:

1. Consulte el número máximo de VLANs soportadas por el switch. Suponga que el switch soporta 250 VLANs. Si al verificar esta información VTP informa que estas 250 están activas, entonces, deberá tomar en cuenta que cuatro de estas VLAN (1002 a 1005) activas son reservadas para redes Token Ring y FDDI.

2. Las VLANs en el rango normal se identifican con un número que va de 1 hasta1001.

3. La configuración de VLANs en el rango normal se encuentra almacenada en el archivo vlan.dat. Si VTP está en el modo transparente, ambas configuraciones; VLAN y VTP se guardan automáticamente en el archivo de configuración de arranque del switch.

4. Si VTP se encuentra en el modo transparente (y el switch ejecuta la versión EI), el switch soportará también VLANs en el rango extendido y como se mencionó anteriormente éstas no serán almacenadas en la base de datos.

5. Antes de crear una VLAN, debe configurar VTP en el modo transparente o modo servidor, si configura VTP en el modo servidor se verá obligado a definir un nombre de dominio VTP, ya que de no hacerlo, éste no funcionará.

6. La serie Catalyst 2950 no soporta el intercambio de tramas Token Ring o FDDI, pero si propaga VLANs a través de VTP.

7. El switch soporta 64 Spanning Trees, y si un switch tiene más VLANs activas que las soportadas por STP, este protocolo permanecerá activo para las 64 soportadas y deshabilitado para las restantes. Si tiene utilizados todos los STPs disponibles y crea otra VLAN en cualquier parte del dominio, Spanning Tree quedara inactivo para esta nueva VLAN.

   Si la lista predeterminada de permisos del puerto se encuentra habilitada en el enlace troncal del switch, la nueva VLAN será transportada por todos los puertos troncales. Y dependiendo del tipo de topología de la red, pueden presentarse bucles infinitos, particularmente si existen switches adyacentes que estén funcionando sin Spanning Tree.

   Afortunadamente, esto puede prevenirse ajustando la lista de permisos del puerto troncal. Si la cantidad de VLANs soportadas en el switch, excede el numero de Spaning Trees, se recomienda configurar el Múltiple STP (IEEE 802.1s) para mapear diversas VLANs a un solo STP.

4.4 Opciones de Configuración

Puede configurar VLANs en el rango normal utilizando cualquiera de los modos siguientes:

- Configurar VLANs con el modo **config – valn**
- Configurar VLANs con el modo **valn configuration**

Cada modo de configuración presenta características particulares que se describen en las próximas secciones.

4.4.1 Modo config - vlan

Para acceder al modo **config-valn**, en el modo de configuración de interfaz debe ingresar el comandol ***vlan***, después seleccione algún identificador de VLAN valido (VLAN ID). Si desea crear una VLAN ingrese un nuevo ID o seleccione alguna existente para modificarla en la base de datos. Puede utilizar la configuración predeterminada o ingresar múltiples comandos para crear una nueva. Una vez terminada la configuración, debe salir de este modo para que las funciones indicadas tomen efecto en el switch.

Para consultar la nueva configuración utilice el comando **show vlan** en el modo privilegiado. Además, debe tener en mente que este modo permite crear VLANs en el rango extendido, siempre y cuando sean soportadas por el switch.

4.4.2 Modo VLAN configuration

Para acceder a este modo de configuración, en el modo privilegiado ingrese el comando **vlan database**. Entonces, escriba el comando ***vlan*** con un nuevo ID para crear una VLAN o seleccione un ID existente. Al igual que en el modo anterior, puede utilizar alguna configuración predeterminada o construir una nueva ingresando múltiples comandos.

Cuando la configuración se encuentre terminada, deberá ingresar el comando ***apply*** o ***exit*** para que la configuración se ejecute. Si ingresa ***exit***, todos los comandos utilizados en la configuración se aplicarán y la configuración actualizará la base de datos. Los avisos VTP serán enviados a

otros switches en el dominio VTP y el indicador del modo privilegiado aparecerá en pantalla del emulador.

4.4.3 Guardar la Configuración VLAN

Como se describió en las secciones anteriores, la configuración de VLANs en el rango normal es almacenada en la base de datos. Si VTP esta configurado en el modo transparente, la configuración se guardará en el archivo de ejecución del switch, si éste es el caso, puede ingresar el comando **copy running-config startup-config** para guardar la configuración en el archivo de arranque del switch.

Cuando guarda la información VLAN ó VTP (incluyendo la información de configuración de VLANs en el rango normal) en el archivo de arranque y reinicia el switch, la configuración quedará determinada de acuerdo a alguno de los casos siguientes:

a. Si en el archivo de configuración de arranque del switch VTP se encuentra en el modo transparente, y el nombre de dominio de VTP en la base de datos es diferente en el archivo de arranque, la base de datos será ignorada por el switch y esté utilizará la información VLAN o VTP que se encuentre en el archivo de arranque.
b. Si el nombre VTP ó el nombre de dominio, son diferentes tanto en el archivo de arranque como en la base de datos para las primeras 1005 VLANs, el switch utilizará el nombre de dominio y modo VTP que encuentre en la base de datos.
c. Si VTP esta en el modo servidor, el nombre de dominio y la configuración VLAN utilizada por el switch para las primeras 1005 VLANs, será tomada de la base de datos.
d. Si el switch está funcionando con la versión IOS 12.1 o una posterior, y utiliza un archivo de arranque antiguo para iniciar el switch, el

archivo de configuración no contendrá la información VTP o VLAN, y el switch utilizará la configuración de la base de datos.

4.4.4 Configuración VLAN predeterminada

La tabla 4.1 muestra la configuración predeterminada para las VLANs Ethernet.

Parámetro	Valor Predeterminado	Rango
Identificador de VLAN	1	1 a 4094 cuando el EI esta instalado y 1 a 1005 para el SI
Nombre de la VLAN	VLAN xxx, donde xxx representa un numero de 4 dígitos igual al valor del ID	Sin rango
Identificador de seguridad 802.10	100001	1 – 4294967294
MTU	1500 Bytes	1500 – 18910 Bytes
Puente de transición 1	0	0 -1005
Puente de transición 2	0	0 – 1005
Estado de VLAN	activo	Activo, suspendido
SPAN remoto	deshabilitado	Habilitado y deshabilitado

Tabla 4.1 Configuración defecto para una VLAN Ethernet

4.5 Creación de una VLAN Ethernet

Cada VLAN Ethernet posee un identificador único de cuatro dígitos, el cual puede ser un número de 1 a 1001 (en el rango normal). Para crear una VLAN en el rango normal y que esta VLAN sea registrada en la base de datos, debe asignarle un número y nombre.

Como se describió en la sección 4.4, “Opciones de configuración”, existen dos métodos para crear VLANs. Cada uno contiene características que difieren unas de las otras. Por esta razón, se describirá el proceso de configuración de VLANs en cada método.

4.5.1 Configurar una VLAN en el modo *config-vlan*

Para crear o modificar una VLAN Ethernet utilizando el modo **config-vlan**, ingrese al modo privilegiado y lleve a cabo las acciones siguientes:

1. Para ingresar al modo de configuración global escriba el comando **configure terminal**, tal como se muestra en la figura 4.1.

2. Ingrese el comando **`vlan`** *vlan-id*, donde *vlan-id* representa el número de identificación para la VLAN. Al realizar esta acción entrará al modo config-vlan. Si desea crear una VLAN, deberá ingresar un nuevo ID. Para modificar alguna VLAN que ya se encuentre en la base de datos, seleccione un identificador existente. En la figura 4.1 se muestra la creación de una VLAN con un identificador igual a 10.

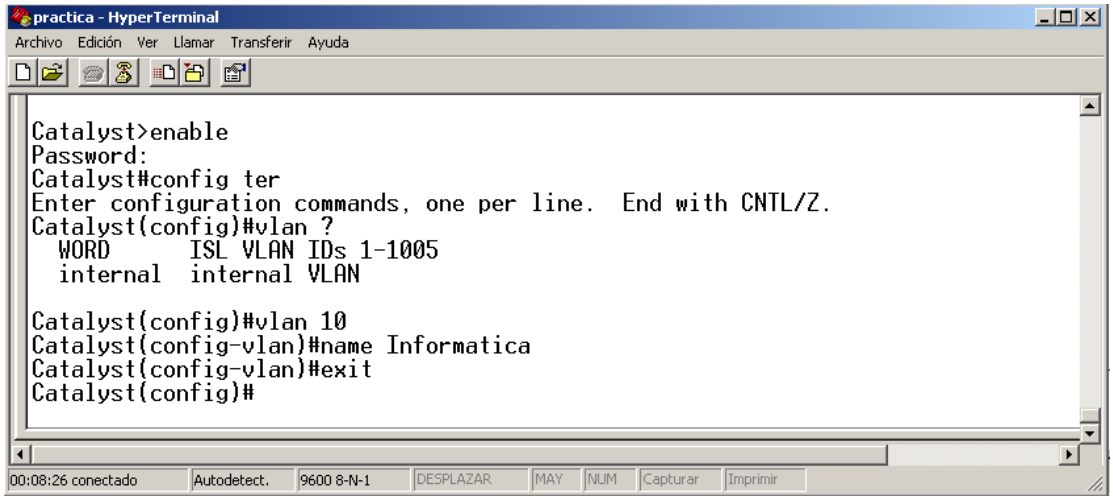


Figura 4.1 Para ingresar al modo **vlan-config**, escriba el comando **vlan**

3. Después, utilice el comando **name** *vlan-name* para nombrar la VLAN, donde *vlan-name* representa el nombre seleccionado para la VLAN. Si no ingresa ningún nombre para la VLAN, por defecto aparecerá la palabra VLAN seguida de un conjunto de dígitos. La figura 4.2 muestra el resultado del comando **show vlan brief**, en esta figura se observa que para una VLAN con un ID igual a 5 (a la cual no se asignó un nombre), el campo predeterminado será VLAN0005.

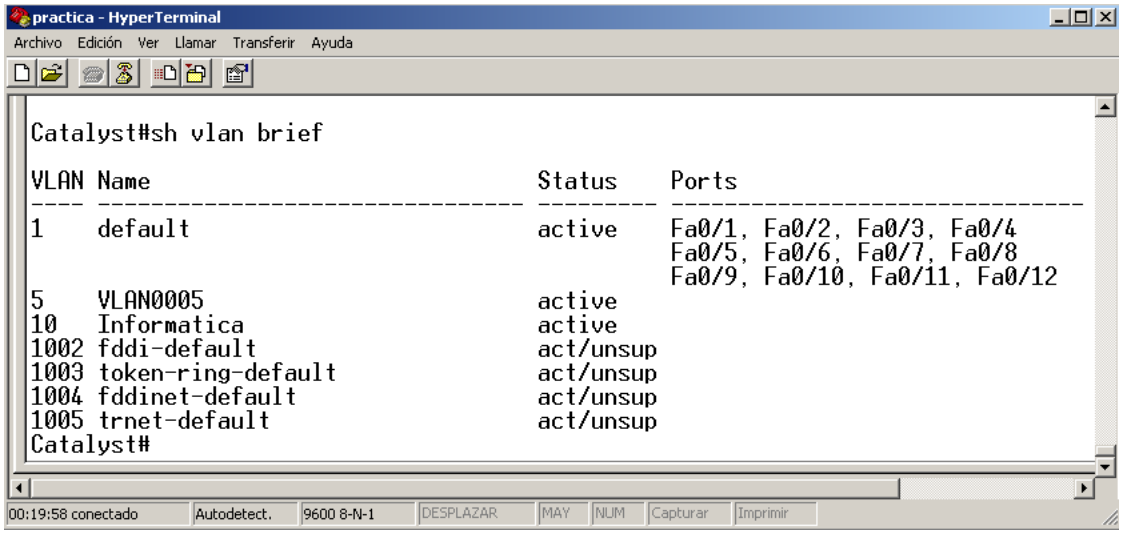


Figura 4.2 Asegúrese de establecer un nombre para cada VLAN

4. En caso de ser necesario puede modificar el tamaño de la unidad de transmisión, para ello, utilice el comando **mtu** *mtu-zise*. Esto le permitirá cambiar el tamaño de la MTU y otras características de la VLAN.

5. De manera opcional, puede configurar una VLAN a través de una sesión remota, Remote Switch Port Analyzer (RSPAN).
6. Una vez ajustados los parámetros a configurar, debe regresar al modo privilegiado EXEC. Para ello, escriba el comando **exit**, tal como se observa en la figura 4.1.

7. Una acción muy importante después de realizar la configuración, consiste en verificar los ajustes realizados. Para revisar la configuración establecida escriba alguno de los comando de análisis siguientes:
   - show vlan {name *vlan-name*}
   - show vlan brief.

   Los resultados de estos comandos se muestran en la figura 4.3. Por lo tanto, el comando a elegir dependerá de la información que necesite consultar.

8. Si VTP se encuentra en el modo transparente, la configuración de la VLAN será almacenada en el archivo de configuración y en la base de datos. Para guardar la configuración en el archivo de arranque del switch, en el indicador de línea escriba el comando **Copy running-config startup-config.** Antes de guardar la configuración es conveniente consultar el estado de la interfaz (o interfaces) en el switch, para esto en el modo privilegiado escriba el comando show running-config. La figura 4.4 muestra los resultados de este comando.

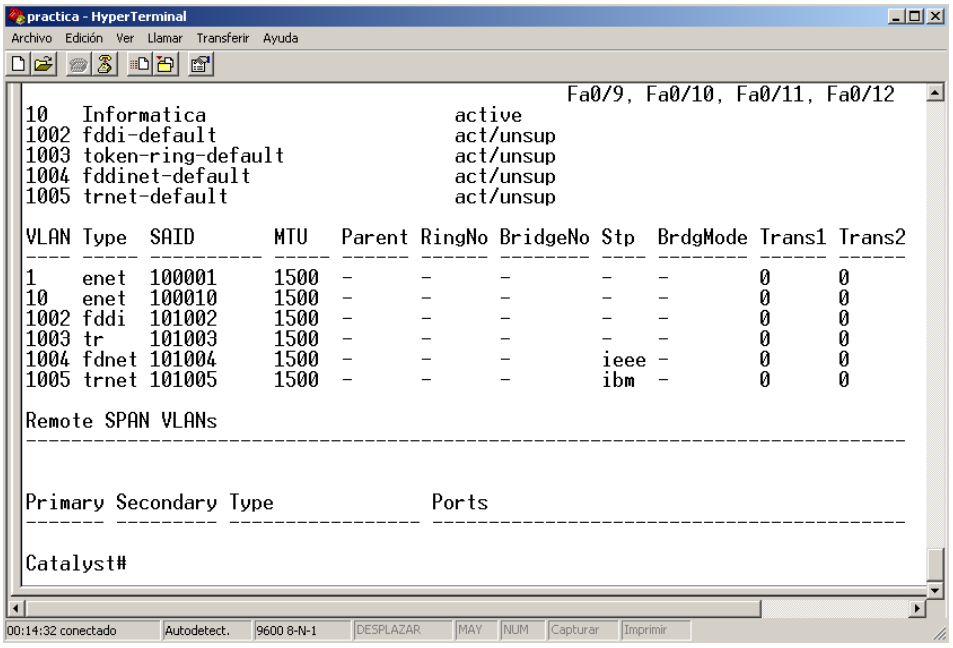

practica - HyperTerminal
Archivo Edición Ver Llamar Transferir Ayuda
Fa0/9, Fa0/10, Fa0/11, Fa0/12
10 Informatica active
1002 fddi-default act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default act/unsup
VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
1 enet 100001 1500 - - - - - 0 0
10 enet 100010 1500 - - - - - 0 0
1002 fddi 101002 1500 - - - - - 0 0
1003 tr 101003 1500 - - - - - 0 0
1004 fdnet 101004 1500 - - - ieee - 0 0
1005 trnet 101005 1500 - - - ibm - 0 0
Remote SPAN VLANs
Primary Secondary Type Ports
Catalyst#
00:14:32 conectado
Autodetect.
9600 8-N-1
DESPLAZAR
MAY
NUM
Capturar
Imprimir

Figura 4.3 El comando Show **vlan** muestra información más detallada acerca de la configuración VLAN en el switch

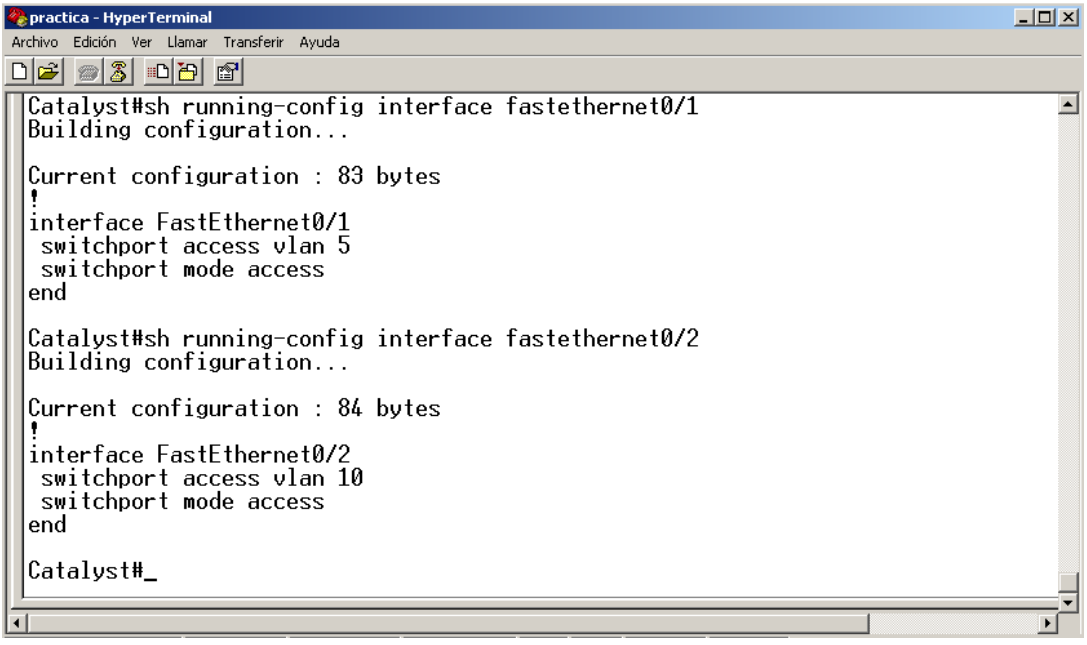


Figura 4.4 El comando **show running-config** muestra la configuración para las interfaces del switch que han sido configuradas.

Para regresar a los valores predeterminados de VLAN (indicados en la tabla 4.1) utilice los comandos siguientes:

- **No vlan name**
- **No vlan mtu**
- **No remote span**

4.5.2 Configurar una VLAN en el modo *VLAN configuration*

Para crear una VLANs o modificar alguna existente utilizando este método, primero ingrese al modo privilegiado y realice los pasos que se mencionan a continuación:

1. El primer paso consiste en ingresar a la base de datos del archivo de configuración, para realizarlo, escriba el comando **vlan database** y después pulse Intro, el resultado se muestra en la figura 4.5.

2. Después de ingresar el comando anterior y pulsar Intro, se encontrará en el modo **VLAN configuration**. Ahora deberá identificar la VLAN Ethernet, para esto, debe asignar un número de identificación (ID) y un nombre (al igual que en el modo anterior); no olvide que el rango disponible para elegir es de 1 a 1001, esto se debe a que los identificadores de 1002 a 1005 están reservados para redes Token Ring y FDDI. El comando para realizar estas acciones es:
   - **vlan** vlan-id **name** vlan-name, donde
     - *Vlan-id* representa al número de identificación, y
     - *Vlan-name* corresponde al nombre elegido para la VLAN

3. Si así lo requiere, puede modificar el tamaño de la unidad de transmisión, el proceso de selección es diferente al del modo anterior, primero debe identificar la VLAN y posteriormente cambiar las

características de la MTU. La estructura del comando a emplear es la siguiente:

- **`Vlan`** *vlan-id* **`mtu`** *mtu-size* , donde *mtu-size* corresponde al nuevo tamaño de la unidad de transmisión.

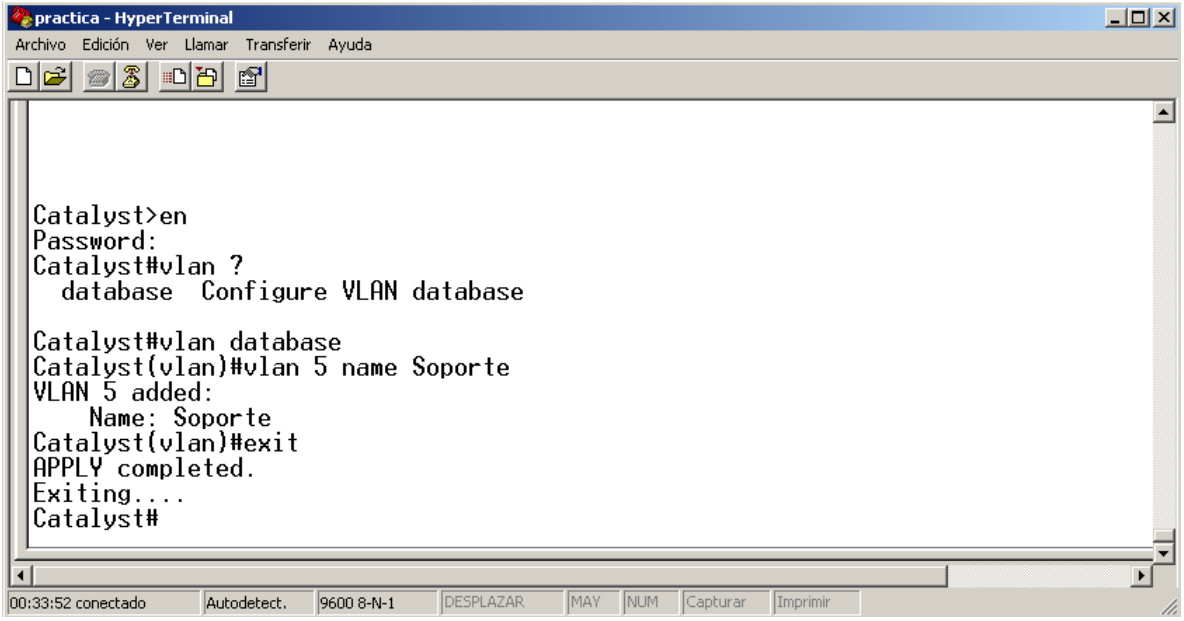


Figura 4.5 En el modo vlan database la asignación se realiza en una sola línea

4. Para actualizar la base de datos VLAN (con la VLAN recientemente creada), propagar esta información por todo el dominio VTP (en caso de estar habilitado en el switch) y regresar al modo privilegiado EXEC, debe escribir en la línea el comando **`exit`** (no olvide pulsar Intro). Como puede observar en la figura 4.6 el sistema arrojará un mensaje indicando que la configuración ha sido aplicada.

5. Después de haber realizado la configuración es conveniente revisar los ajustes, de esta manera podrá comprobar que los parámetros ingresados o modificados son los correctos. Para verificar la configuración establecida en el switch, utilice alguno de los comandos siguientes:

- **show vlan** {name / id *vlan-id*}
- **show vlan brief**

En este caso el comando empleado es **show vlan brief,** el resultado se muestra en la figura 4.6.

6. Si VTP se encuentra en modo transparente, la configuración de la VLAN será guardada en el archivo de ejecución y en la base de datos. Para guardar la configuración de la VLAN en el archivo de arranque del switch, utilice el comando ***copy running-config startup-config***, no olvide que antes puede revisar la configuración de ejecución.

Si compara los procedimientos de configuración de VLANs de los métodos anteriormente descritos, observará que en el modo VLAN configuration (configuración en la base de datos) no es posible configurar una sesión RSPAN .

4.6 Asignación de puertos de acceso estático una VLAN

Como se explicó, es posible asignar puertos que permanezcan fijos (estáticos) a una VLAN, estos puertos permanecerán con la configuración establecida hasta que el administrador de la red decida modificarla, ya sea para asignarlos a una VLAN o a otro dominio de difusión. En este tipo de asignación (membresía), VTP puede difundir la información asociada al puerto por todo el domino, para que VTP no propague estas difusiones por la red, debe ajustarlo al modo transparente, es decir, debe ser deshabilitado.

Si por alguna razón, asigna determinada interfaz a una VLAN que no exista en la base de datos del switch, el sistema creará la nueva VLAN y se difundirá por todo el dominio de administración.

Para llevar a cabo la asignación de puertos a una VLAN o grupo de VLANs, primero, debe ingresar al modo privilegiado (superando el proceso de autenticación en el switch) y realizar los pasos que se detallan a continuación.

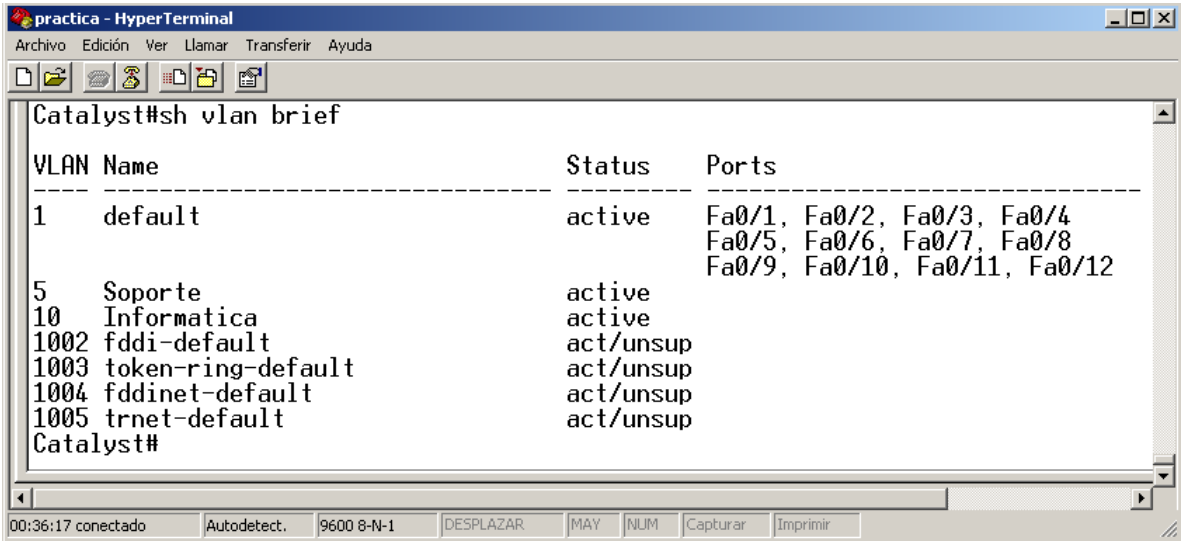


Figura 4.6 Resultado del comando **show vlan brief** para el modo **vlan database**

1. Cuando se encuentre ubicado en el modo privilegiado de la CLI, debe acceder al modo de configuración global mediante el comando **configure terminal**.

2. Ahora, deberá seleccionar la interfaz que será asignada a la VLAN. Para ello, escriba el comando **Interface** *interface-id*, donde, *interface-id* representa el identificador de la interfaz elegida, el resultado se muestra en la figura 4.7.

3. Después de seleccionar la interfaz, tiene que definir el modo de membresía que otorgará al puerto, para el caso de asignación estática debe seleccionar el **modo de acceso,** este modo mantendrá

permanentemente al puerto en el modo no-trunking (inactivado para el trunking).

4. Hasta este momento ya definió la interfaz y el modo de membresía del puerto, el siguiente paso consiste en determinar la VLAN a la que pertenecerá este puerto. Para realizar la asignación del puerto a la VLAN utilice el comando **Switchport access vlan** *vlan-id.*, el resultado se muestra la figura 4.7.

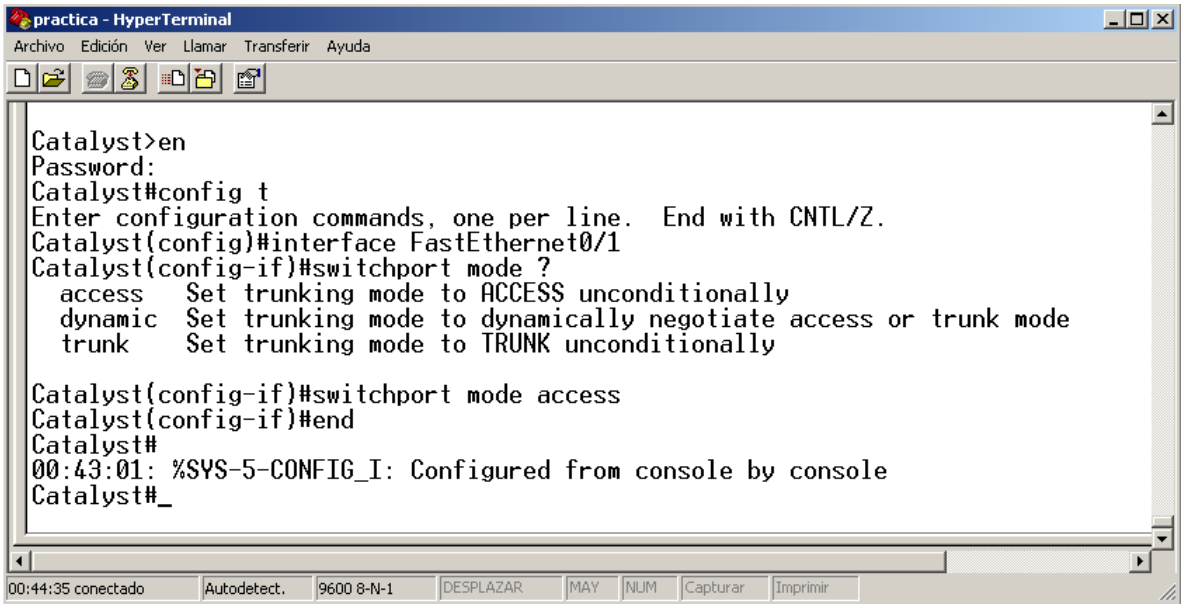


Figura 4.7 Asignación de puerto de acceso estático a una interfaz

5. Como podrá observar solo puede asignar una interfaz por línea a una VLAN, por lo tanto, si requiere asignar más puertos a dicha VLAN, deberá repetir los pasos hasta ahora descritos. La figura 4.7 muestra la asignación de puertos de acceso estático a diferentes VLANs. No olvide que todos estos pasos fueron realizados en el modo de configuración global, por lo que al terminar la configuración debe regresar al modo Privilegiado EXEC.

6. Después de terminar la configuración de la VLAN, es recomendable realizar una revisión de la misma, de esta manera, puede comprobar que los parámetros configurados son los correctos. Para verificar la configuración establecida en el switch utilice alguno de los comandos de análisis siguientes:

   - **show running-config interface** *interface-id*. Este comando permite verificar el modo de membresía asignada a la interfaz.

   - **show interfaces** *interface-id* **switchport.** Verifica la configuración en el modo administrativo y muestra los campos de modo de acceso. Las figuras 4.4 y 4.8 muestran los resultados de estos comandos.

7. Guarde los ajustes realizados en el archivo de configuración.

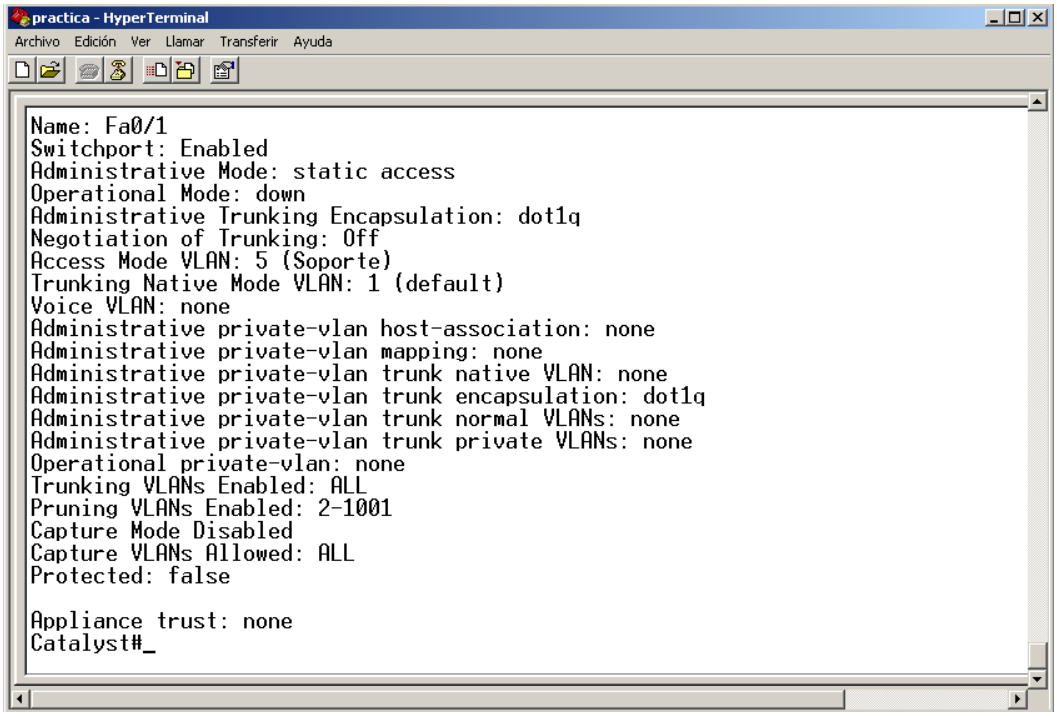


Figura 4.8 Resultado para el comando **show interfaces** *interface-id* **switchport**

4.7 Configuración de VLANs en el rango extendido

Cuando VTP está en el modo transparente y el **EI** se encuentra instalado, puede crear VLANs en el rango extendido (de 1006 a 4094). Estas VLANs habilitan servicios que permiten incrementar la infraestructura de la red y aumentar el número de usuarios. Sin embargo, como lo muestra la figura 4.1 el switch 2950 solo soporta VLANs con identificadores de 1 a 1005. Esto debido a que ejecuta la versión **SI** del IOS.

Para la serie 2950 no es posible implementar VLANs en el rango extendido. Como se muestra en la figura 4.9, si intenta crear una VLAN con algún identificador no valido, el sistema arrojará un mensaje de error y ésta no será creada en la base de datos. No obstante, en las secciones siguientes se describe el procedimiento que deberá utilizar para crear VLANs en el rango extendido.

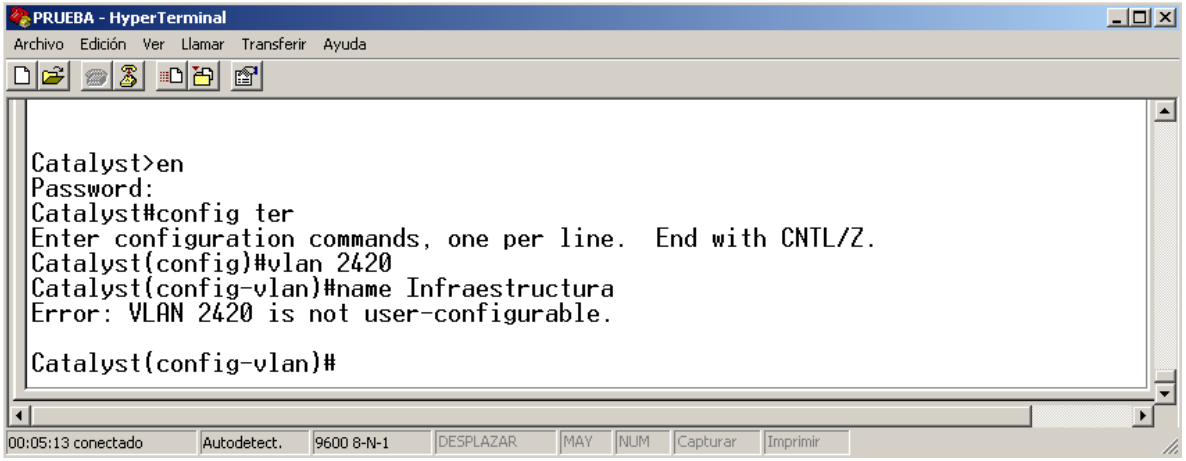


Figura 4.9 Debe asegurarse que el identificador seleccionado se encuentre en el rango disponible

Para configurar VLANs en el rango extendido utilice siempre el modo config-vlan (al cual accede ingresando el comando de configuración global **vlan** *vlan-id*), ya que el rango extendido no es soportado en el modo VLAN database.

Debido a que VTP se encuentra en el modo transparente, las configuraciones de VLAN en el rango extendido no son registradas en el archivo vlan.dat, éstas se guardan en el archivo de ejecución del switch. Para que pueda guardar la configuración en el archivo de arranque del switch, debe utilizar el comando **copy running-config startup-config** en el modo privilegiado EXEC.

4.7.1 Guía de configuración

Cuando realice la configuración de una VLAN en el rango extendido tome en cuenta las consideraciones siguientes:

a. Para añadir una VLAN en el rango extendido tiene que utilizar el comando de configuración global **config-vlan** y acceder al modo config-vlan.
b. Los identificadores de VLAN no son almacenados en la base de datos, por lo que no son reconocidos por VTP.
c. En la lista de reducción de VTP (pruning eligible list) no puede incluir VLANs configuradas en el rango normal.
d. Cuando configure VLANs en el rango extendido, VTP debe ajustarse al modo transparente. Si éste no es el caso y VTP se encuentra en el modo cliente o servidor, se producirá un mensaje de error, y la VLAN será rechazada.
e. Puede ajustar VTP al modo transparente en ambos modos de configuración; modo de configuración global (config-vlan) y modo de configuración VLAN database. Guarde su configuración en el archivo de arranque, de esta manera cuando inicie el switch, VTP se encontrará en el modo transparente. De lo contrario, perderá la configuración de la VLAN.

f. Las VLANs en el rango extendido no pueden ser configuradas por VMPS.
g. El protocolo Spaning Tree se encuentra habilitado por defecto sobre el rango extendido, pero puede deshabilitarlo utilizando el comando de **no spaning-tree vlan**. Cuando el número máximo de STPs (64) se encuentran utilizados en el switch, Spaning Tree será deshabilitado en cualquier VLAN que sea creada. Si el número de VLANs excede el número máximo de STPs, se recomienda que configure MSTP para mapear múltiples VLANs a un solo STP. Desafortunadamente, la configuración de MSTP se encuentra fuera de los alcances de este trabajo, por lo cuál, deberá consultar la bibliografía recomendada al final del trabajo.

4.7.2 Configurar una VLAN en el rango extendido

Para crear una VLAN en el rango extendido, en el modo de configuración global escriba el comando **vlan,** después seleccione el número de identificación. Este comando le permitirá ingresar al modo config-vlan. Las VLANs en el rango extendido tienen las mismas características Ethernet predeterminadas que las VLANs configuradas en el rango normal, excepto que el único parámetro que no puede modificar es el tamaño de la unidad de transmisión (MTU).

Si asigna un identificador del rango extendido a una VLAN cuando VTP no se encuentre en el modo transparente, el sistema generará un mensaje de error cuando salga del modo config-vlan y la VLAN que haya configurado no será creada. Recuerde que las VLANs en el rango extendido no son registradas en la base de datos; éstas se almacenan en el archivo de ejecución del switch. Para guardar la configuración de la VLAN en el archivo de arranque, en el modo Privilegiado utilice el comando **copy running-config startup-config**.

Para crear una VLAN en el rango extendido, lleve a cabo los pasos que a continuación se explican:

1. Para ingresar al modo de configuración global, escriba el comando **configure terminal**, recuerde que este modo debe lanzarse desde el modo privilegiado, el cual por cuestiones de seguridad debe estar protegido por contraseña. Para ver el proceso de activación de contraseñas, revise la sección 3.4 “Funciones administrativas”.

2. Recuerde que el switch puede aceptar la configuración de VLANs en el rango extendido, si el protocolo de enlace troncal está configurado en el modo transparente, es decir, deshabilitado. Por lo tanto, el siguiente paso consiste en configurar VTP a este modo, éste proceso es descrito en el anexo C.

3. Después de configurar VTP al modo adecuado, debe ingresar al modo config-vlan. En la línea de comandos escriba el comando **vlan** *vlan-id.*

4. Si a si lo requiere, modifique la VLAN cambiando el tamaño de la MTU, el comando a utilizar es **mtu** *mtu-zise***.** Si utiliza las opciones de ayuda de la interfaz de línea de comandos en el modo config-vlan, es posible que aparezca una lista con muchos comandos, pero solo el comando **mtu** *mtu-zise* es el único soportado para el rango extendido.

5. Después de realizar los ajustes anteriores debe regresar al modo privilegiado, para esto ingrese el comando **end.**

6. Con el comando de **show vlan** *vlan-id* compruebe que la VLAN ha sido creada.

7. Si verifico que la VLAN ha sido creada, es conveniente que guarde la configuración en el archivo de arranque del switch, debe guardar también la configuración de VTP (en el modo transparente). De lo contrario, si el switch es reiniciado, perderá la configuración de VTP a si como los ajustes de la VLAN.

Al igual que en una VLAN del rango normal, también es posible asignar puertos a estas VLANs. El procedimiento empleado para determinar puertos de acceso estático a una VLAN del rango extendido, es el mismo que se describe en la sección 4.7 “Asignación de puertos de acceso estático”.

4.8 Verificando la configuración VLAN

Para ver una lista de todas las VLANs configuradas en el switch, incluyendo las VLANs del rango extendido (en caso de estar soportadas por el switch), use el comando **show vlan** en el modo privilegiado. La lista incluirá el estado de la VLAN, tipo de membresía asignada a los puertos e información general de la configuración. Para ver las VLANs configuradas en el rango normal utilice el comando **show** en el modo VLAN configuration (ingresando el comando **vlan database**). Si desea consultar una lista de los identificadores de las VLAN, use el comando **show running-config vlan** e ingrese el identificador de la VLAN a consultar.

La tabla 4.2 muestra una lista de los comandos que son utilizados para verificar la configuración de VLANs. Para más detalles acerca de los comandos mostrados y explicaciones de los campos de salida, refiérase a la lista de comandos que se encuentra en el anexo A “Referencia de comandos”.

Comando	Modo del comando	Propósito
Show	VLAN configuration	Muestra es estado de las VLANs en la base de datos.
Show current [vlan-id]	VLAN configuration	Muestra el estado de todas las VLAN en la base de datos o de alguna especificada en particular.
Show interfaces [vlan vlan-id]	Privileged EXEC	Muestra las características para una VLAN especificada.
Show running-config vlan	Privileged EXEC	Muestra todas o un rango de las VLANs configuradas en el switch.
Show vlan [id vlan-id]	Privileged EXEC	Muestra todos los parámetros de las VLAN en el switch.

Tabla 4.2 Comandos utilizados para consultar la configuración de VLANs.

4.9 Eliminar una VLAN

Cuando elimina una VLAN de un switch y VTP se encuentra en el modo transparente, la VLAN es borrada de manera automática en la base de datos en todos los switchs del dominio VTP. Por lo contrario, si VTP se encuentra en el modo transparente y elimina una VLAN, ésta será removida solo en el switch donde la elimino.

Recuerde que no puede eliminar las VLANs designadas para otros medios de transmisión (VLAN Ethernet de administración, Token Ring y FDDI). La tabla 4.3 indica los comandos utilizados para eliminar una VLAN del switch.

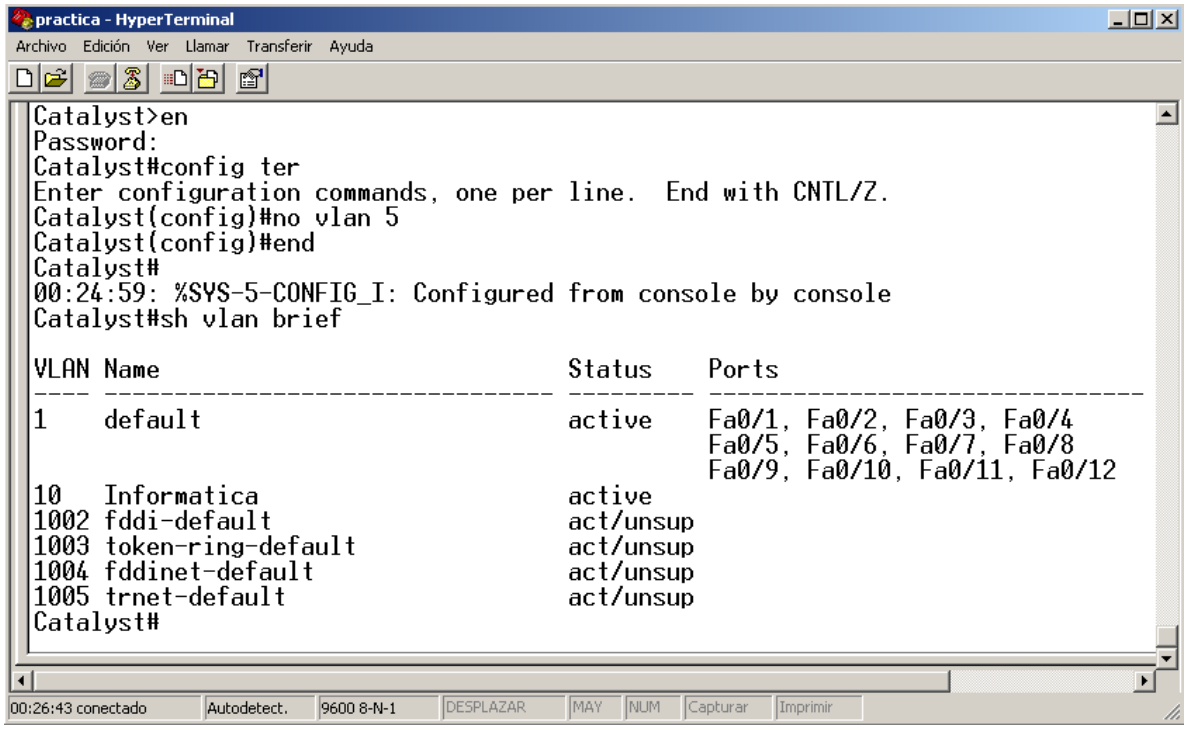


Figura 4.10 Eliminar una vlan

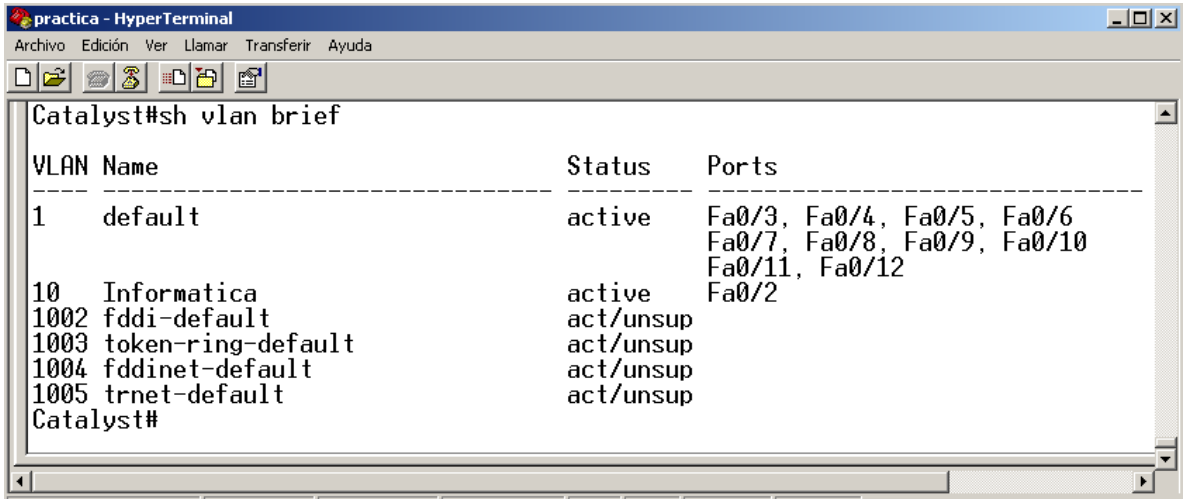


Figura 4.11 Después de eliminar una VLAN, se observa que el puerto 1 permanece inactivo

Paso	Comando	Propósito
1	Configure Terminal	Permite ingresar al modo de configuración global.
2	No vlan vlan-id	Elimina una VLAN indicando su identificador asignado con anterioridad.
3	End	Regresa al modo privilegiado
4	Show vlan brief	Al ingresar este comando podrá asegurarse que la VLAN ha sido removida.
5	Copy running-config vlan-config	Si VTP se encuentra en el modo transparente, la configuración de la VLAN estará guardada en el archivo de ejecución, tanto como en la base de datos. Con este comando guardará la configuración en el archivo de inicio del switch.

Tabla 4.3 Pasos empleados para eliminar una VLAN

Cuando elimina una VLAN (Figura 4.10), todos los puertos asignados a dicha VLAN permanecerán inactivos hasta que sean asignados de nueva cuenta a otra VLAN. En figura 4.11 se observa que la interfaz **FastEthernet0/1** no aparece en la lista de puertos para la VLAN 1, lo que indica que se encuentra inactiva. Para regresar esta interfaz a su estado predeterminado, en el modo de configuración de la interfaz escriba el comando **default interface** *interface-id*.

4.10 Comunicación entre VLANs

En una VLAN, los host pertenecen a un solo dominio de broadcast, los cuales dividen el flujo de tramas en base a la información de capa 2 del modelo OSI. Esta capacidad permite que los host puedan comunicarse libremente entre ellos.

Por defecto, solo los host que sean miembros de la misma VLAN podrán comunicarse. Para permitir que la comunicación entre VLANs sea posible, se necesita de un router o switch que soporte funciones a nivel capa 3.

Como se muestra en la figura 4.12, si la red esta formada por unas cuantas VLANs (dos o cuatro), entonces puede utilizar un router que cuente con la cantidad de interfaces (dos o cuatro) Fast o Gigabit Ethernet necesarias. En la figura 4.14 podemos observar que cada interfaz del router esta configurada como una conexión de acceso hacia los puertos del switch. Con esto podemos determinar que cada dirección IP en estas interfaces, puede ser considerada como el defaul gateway de cada host asignado en alguna VLAN.

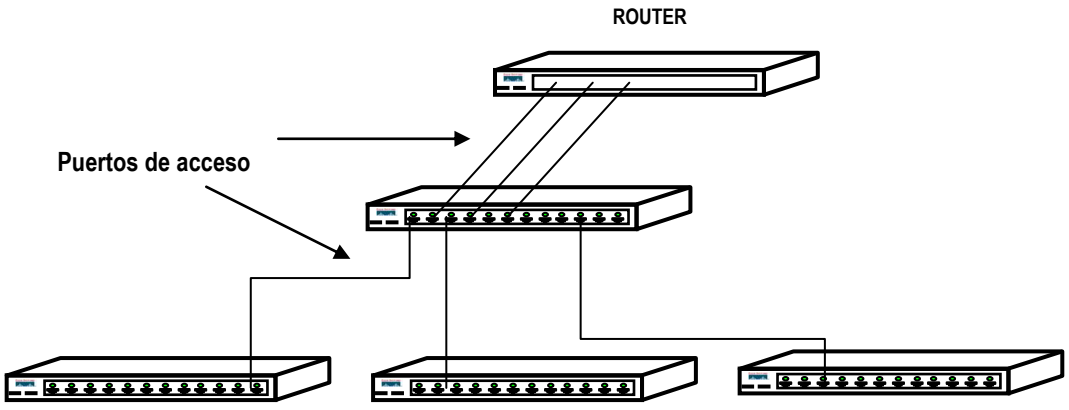


Figura 4.12 Router conectando VLANs mediante varias interfaces.

Si la cantidad de VLANs sobrepasa los puertos disponibles en el router, puede utilizar una sola interfaz para todas estas VLANs, solo tiene que configurarla para que soporte el etiquetado 802.1Q o ISL, en lugar de usar una interfaz para cada VLAN. La figura 4.15 muestra como una interfaz del router es utilizada para permitir la comunicación entre VLANs, este método de enrutamiento es llamado "*router on a stick*."

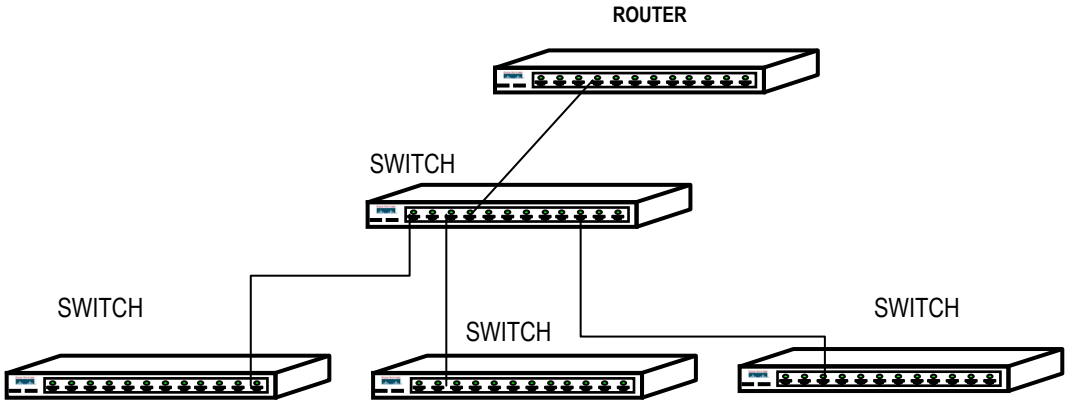


Figura 4.13 Router conectando varias VLANs utilizando solo una interfaz

Realizar la configuración del enrutamiento en un ambiente VLAN, puede convertirse en una labor complicada si se desconocen los temas relacionados con el direccionamiento de capa 3. Para comprender que cada VLAN es una subred separada, debe ser capaz de establecer el direccionamiento IP en cada host conectado a una VLAN y resolver cualquier problema que pudiera presentarse.

Para que alguna interfaz del router; FasEthernet o GigabitEthernet, soporte el enrutamiento ISL o 802.1 Q, debe ser dividida en interfaces lógicas, una para cada VLAN. Tales interfaces son llamadas *subinterfaces.* Para ajustar una interfaz del router al modo troncal, deberá utilizar el comando **encapsulation** y seleccionar el tipo de etiquetado. Tenga en cuenta que los switch catalyst 2950 solo soportan el etiquetado 802.1 Q.

La figura 4.14 muestra una red que utiliza una sola interfaz del router para permitir la comunicación VLAN. Lo primero que debe hacer es identificar las subredes que han sido asignadas a cada VLAN, la tabla 4.4 muestra las direcciones de subred y los rangos de direcciones IP (obtenidos al dividir la dirección 192.168.10.0 utilizando la mascara de subred 255.255.255.224) asignados a cada VLAN. Las direcciones IP asignadas a cada host se encuentran en la tabla 4.5, y corresponden al rango asociado a cada VLAN.

VLAN	Dirección de subred	Dirección de broadcast	Rango de direcciones
1	192.168.10.0	192.168.10.31	192.168.10.1 - 192.168.10.30
2	192.168.10.32	192.168.10.63	192.168.10.33 - 192.168.10.62
3	192.168.10.64	192.168.10.95	192.168.10.65 - 192.168.10.94

Tabla 4.4 Direcciones de subred asignada a cada VLAN

VLAN	Host	Direcciones asignadas
1	A, B	192.168.10.2, 192.168.10.3
2	C, D	192.168.10.34, 192.168.10.35
3	E, F	192.168.10.66, 192.168.10.67

Tabla 4.4 Direcciones IP asignadas a cada host

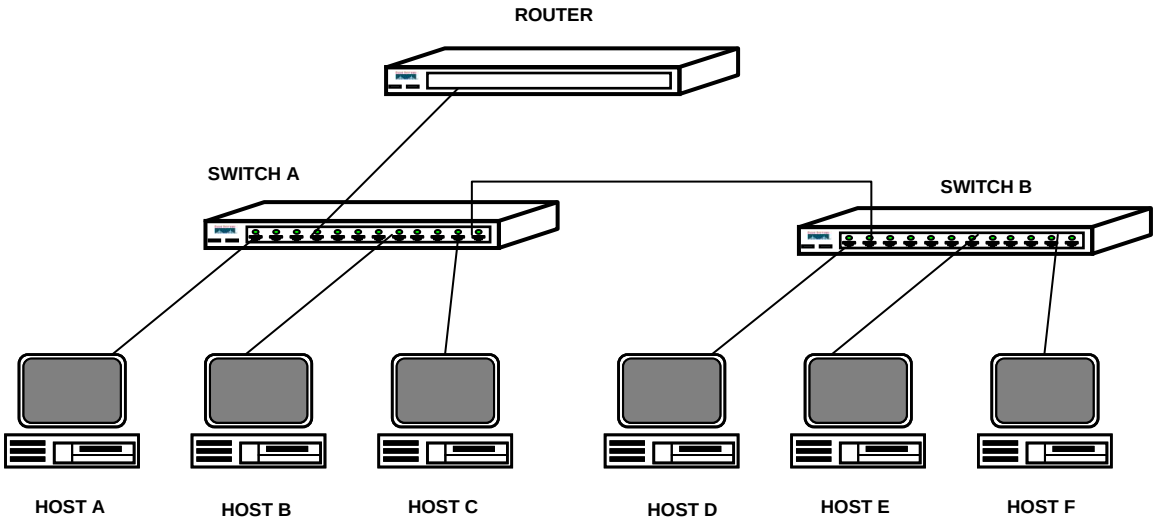


Figura 4.14 Configuración del enrutamiento entre VLANs

El procedimiento empleado para configurar el enrutamiento entre VLANs se describe en los pasos siguientes:

1. Seleccione la interfaz del switch (FastEthernet o GigabitEthernet) que será conectada a la interfaz del router (mediante un cable directo) para proporcionar la comunicación entre VLANs, y configúrela como u puerto troncal.
2. Después de seleccionar las interfaces adecuadas, debe activar la interfaz del router e indicarle que no configurará una dirección IP sobre ésta, ya que no seleccionará ningún protocolo de encaminamiento (al menos para dicha interfaz). La figura 4.15 muestra como se realiza este procedimiento.

3. Como es de observarse en la figura 4.14 la red esta formada por tres VLANs (incluyendo la VLAN de administración), por lo cual, debe dividir la interfaz en tres subinterfaces, para esto, después de activar el puerto en el router, escriba el comando **interfaz** *FastEthernet0/**x.y***, donde **x** representa la interfaz a dividir, y ***y*** la división realizada en tal interfaz.

En este caso se ha asignado la subinterfaz .1 del puerto 0 del router a la VLAN de administración. Al ingresar el comando anterior y pulsar Enter, aparecerá en pantalla el indicador del modo de configuración de subinterfaz.

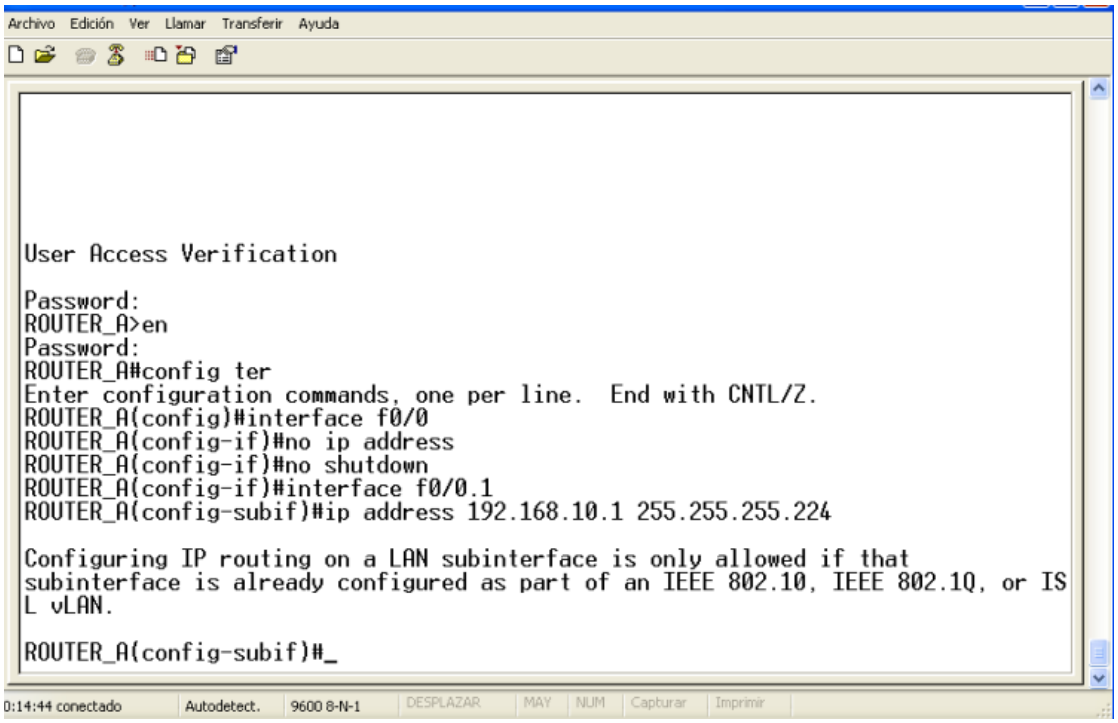


Figura 4.15 Selección de la interfaz del router

4. Mediante el comando **ip address** ip-address, asigne una dirección IP a esta interfaz, la dirección debe estar en el rango establecido para la VLAN en cuestión. En la figura 4.15 se ha asignado la primera dirección IP de la subred 0, la cual será el default gateway para los host que pertenezcan a dicha VLAN. Aparecerá un mensaje indicándole que el ruteo IP se realizará en esta subinterfaz, solo si dicha subinterfaz es parte de un enlace troncal 802.1 Q o ISL.

5. Ahora debe configurar el tipo de encapsulamiento en la subinterfaz, en indicador escriba ? para verificar los tipos de encapsulamiento

soportados por el switch, la opción dot1Q, corresponde etiquetado 802.1 Q. La figura 4.18 muestra como se utiliza el comando **encapsulation** *id* para seleccionar el tipo de etiquetado. El identificador *id* debe ser igual al ID de la VLAN asignada a la subinterfaz. Observe que los identificadores corresponden a los valores establecidos para las VLANs creadas en el rango extendido.

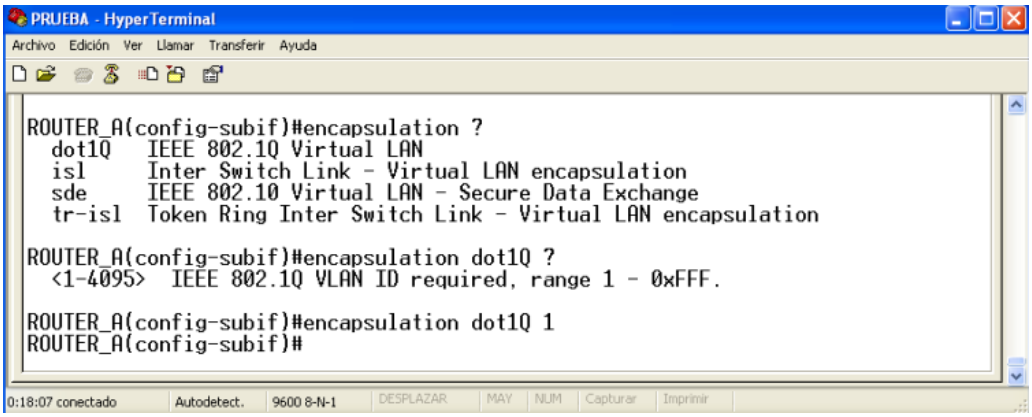


Figura 4.16 Seleccione el etiquetado soportado en el switch

6. En la figura 4.17 se muestra la asignación de subinterfaces a las VLANs restantes, como es de observarse, el procedimiento es el mismo que el utilizado con anterioridad.

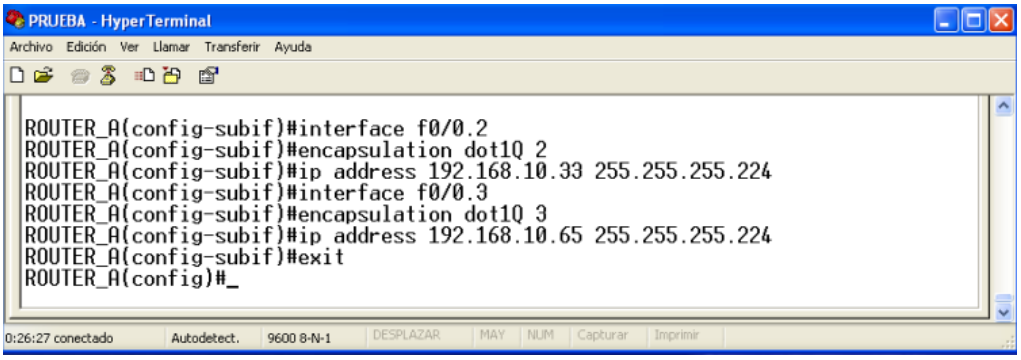


Figura 4.17 Asignación de subinterfaces a las VLANs 2 y 3

7. Para verificar la configuración realizada en la interfaz, utilice el comando show, el resultado se muestra en la figura 4.18.

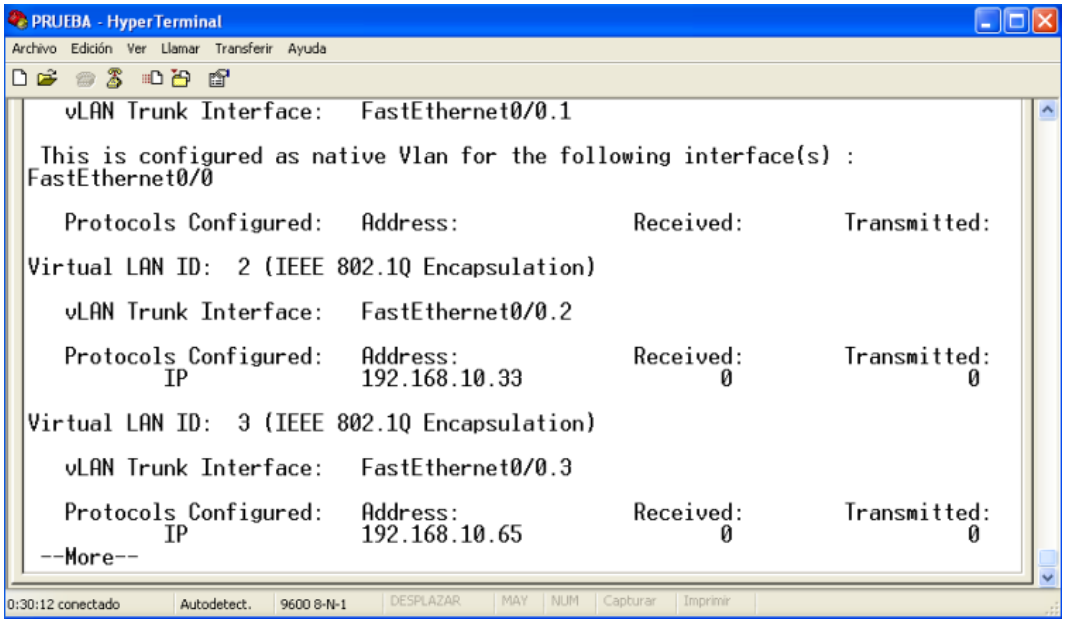


Figura 4.18 Verifique la configuración realizada en la interfaz

Preguntas de repaso

28. Diga cuales son las consideraciones que debe tomar en cuenta antes de configurar una VLAN.
29. Explique por que las VLANs son asociadas con subredes IP.
30. De una explicación de cada uno de los modos de membresía VLAN a los que puede ser asociada una interfaz del switch.
31. Indique cual es la diferencia entre una VLAN creada en el rango normal y otra creada en el rango extendido.
32. Explique por que es necesario activar VTP en switch cuando crea VLANs.
33. Diga cuales son los parámetros que puede ajustar cuando configura VLANs.
34. Explique que sucede cuando la cantidad de VLANs creadas en el switch excede el número de Spanning Trees soportados.
35. Explique como se comporta el switch cuando VTP se encuentra en el modo transparente y el nombre de dominio no corresponde al indicado en el archivo de arranque del switch.
36. Indique cuales son los comandos utilizados para realizar la consulta de VLANs y explique sus diferencias.
37. Explique como se comporta el switch cuando el modo y dominio VTP son diferentes en los archivos vlan.dat y arranque.
38. Diga cual debe ser la configuración de VTP cuando crea VLANs en el rango extendido.
39. Explique que sucede cuando elimina una VLAN del switch y VTP se encuentra en alguno de los modos transparente o servidor.
40. Indique cuales son los parámetros que puede ajustar cuando crea una VLAN en el rango extendido.
41. Explique cuales son las funciones de la VLAN de administración.
42. Explique por que es necesario un dispositivo con capacidad de capa 3 para proporcionar la comunicación entre VLANs.

Práctica 4.1 Creación de VLANs

Como recordara, existen tres tipos de VLANs; estáticas, dinámicas y de puerto central. Dependiendo del modelo del switch que utilice, dispone de dos modos de configuración; modo config vlan y modo vlan data base.

En está práctica realizará la configuración de VLANs estáticas en un switch de la serie 2950. Así como también, asignará puertos de acceso a cada VLAN. Para ello, deberá seguir paso a paso los procedimientos descritos en las secciones 4.6 y 4.7.

1. Construya una red como se muestra en la figura 4.19.

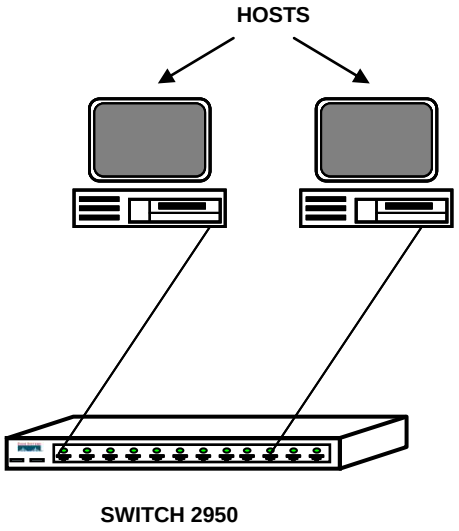


Figura 4.19 Red formada por dos host y un switch

2. Seleccione una dirección IP (clase A, B, o C) y divídala en subredes. Si desconoce este proceso, puede utilizar las direcciones IP descritas en la tabla 4.4. En la cual se ha divido la dirección 192.168.10.0 en subredes de acuerdo a la mascara 255.255.255.224 (/27).

3. Configure la dirección IP y el default gateway en el switch y los host. Las direcciones seleccionas deben estar en la misma subred. Haga ping a cada dirección IP; de host a host, de host a switch y de switch a host. Asegúrese que estos sean satisfactorios.
4. Cree dos VLANs y asígneles un nombre. El switch Cisco 2950 solo soporta VLANs en el rango normal, por lo que deberá elegir un identificador comprendido en el rango 1 a 1001. No olvide que el rango normal es soportado por ambos modos de configuración (vlan configuration y vlan database).

Dirección de subred	Dirección de broadcast	Rango de direcciones
192.168.10.0	192.168.10.31	192.168.10.1 - 192.168.10.30
192.168.10.32	192.168.10.63	192.168.10.33 - 192.168.10.62
192.168.10.64	192.168.10.95	192.168.10.65 - 192.168.10.94
192.168.10.96	192.168.10.127	192.168.10.97 - 192.168.10.126
192.168.10.128	192.168.10.159	192.168.10.129 - 192.168.10.158
192.168.10.160	192.168.10.191	192.168.10.161 - 192.168.10.190
192.168.10.192	192.168.10.223	192.168.10.193 - 192.168.10.222
192.168.10.224	192.168.10.255	192.168.10.225 - 192.168.10.254

Tabla 4.6 División en subredes de la dirección 192.168.10.0

5. Verifique la configuración establecida, puede emplear los comandos show vlan y show vlan brief. Ambos comandos deberán mostrar activa la VLAN de administración y las interfaces asociadas a ella.

6. Asigne al menos dos interfaces a cada VLAN, debe dejar puertos disponibles en la VLAN de administración, de lo contrario no podrá efectuar pruebas de conexión con los host. Después de realizar esta acción, ingrese el comando show vlan brief y complete la tabla 4.7. Por defecto todos los puertos pertenecen a la VLAN natural, por lo que solo tiene que asignar puertos a las VLANs restantes.

Nombre de la VLAN	Identificador	Interfaces asignadas
Administración	1	
	2	
	3	

Tabla 4.7 Determine los puertos que asignará a cada VLAN

7. Ahora que ha creado las VLANs, en la tabla 4.8 registre la subred a la que pertenecerá cada una.

Nombre de la VLAN	Sudred	Rango de direcciones
Administración		

Tabla 4.8 Determine la subred que asignará a cada VLAN

8. Configure nuevamente cada host con alguna dirección IP de la subred asignada a la VLAN 1. Después conecte cada host en algún puerto asignado a está VLAN. Posteriormente, utilice el comando ping para verificar la conexión entre ambos host y el swith. Los resultados de las pruebas de conexión deben ser satisfactorias ya que los host se encuentran en la misma VLAN.

9. Configure nuevamente cada host con alguna dirección IP de la subred asignada a la VLAN 2 (o al identificador elegido). Después conecte cada host en algún puerto asignado a esta VLAN. Posteriormente, utilice el comando ping para verificar la conexión entre ambos host y el swith. Los resultados de las pruebas de conexión deben ser satisfactorias ya que los host se encuentran en la misma VLAN.

10. Ahora conecte cualquier host en algún puerto que no pertenezca a la VLAN 2, utilice el comando ping para verificar la conexión entre ambos host. Los resultados de las pruebas de conexión deben ser insatisfactorias, ya que los hosts se encuentran en VLANs diferentes.

CAPITULO V

DESCRIPCION DE LOS ENLACES TRONCALES

5.1 El enlace troncal

Un enlace troncal es una conexión punto a punto entre una o más interfaces Ethernet de un switch a otro dispositivo como un router o un switch. Los enlaces troncales; Fast Ethernet y Gigabit Ethernet, transportan tramas de múltiples VLANs sobre una sola conexión. Esto permite difundir la VLAN por toda la red. La figura 5.1 muestra una red formada por tres switches y un router que están conectados por medio de enlaces troncales.

Puede configurar un enlace troncal en una interfaz o sobre un grupo de interfaces. Las interfaces Ethernet pueden soportar diferentes modos de enlace troncal; estos modos se encuentran indicados en la tabla 5.1. Es posible ajustar una interfaz para que participe como enlace troncal, aunque si lo prefiere, puede configurar la interfaz para que establezca negociaciones con otras interfaces. Si este es el caso, las interfaces deben estar en el mismo dominio VTP.

Antes de crear una VLAN, debe decidir si utilizará VTP para difundir tramas en la red. Por este motivo, es necesario conocer el procedimiento empleado para activar VTP al modo correspondiente. El anexo C describe las características de este protocolo y los comandos empleados para su configuración.

La negociación del enlace troncal es controlada por DTP (Dinamic Trunking Protocol), el cuál es un protocolo punto a punto. Sin embargo, algunos dispositivos de red pueden enviar tramas DTP inadecuadamente, ocasionando errores en la configuración de los equipos. Para evitar esto, las interfaces que no soporten este protocolo, deben ser configuradas para que no envíen tramas DTP por todo el dominio.

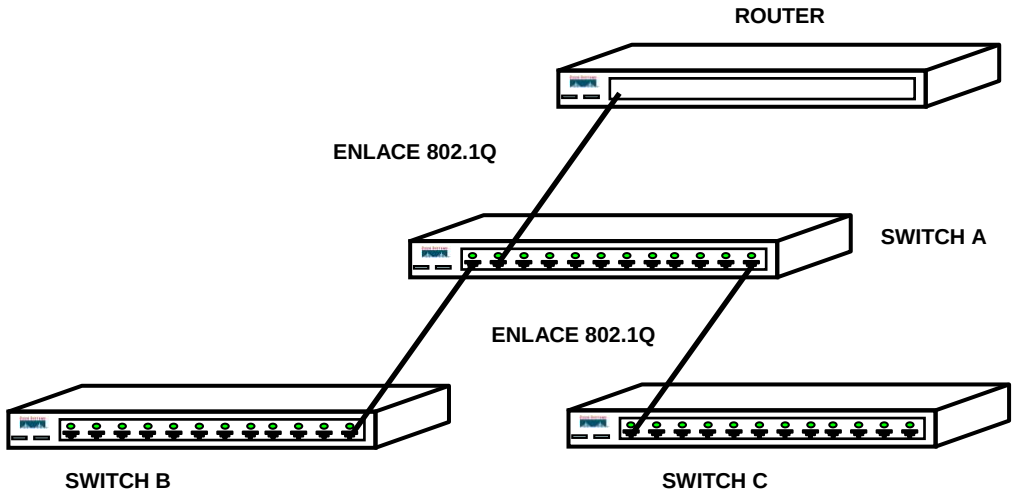


Figura 5.1 Red conectada por medio de enlaces troncales 802.1Q

5.1.1 Funcionamiento del enlace troncal

Las tablas de conmutación construidas por los switches se usan para tomar decisiones de envío sobre un enlace troncal; tomando en cuenta las direcciones MAC destino de las tramas. A medida que aumenta la cantidad de VLAN que viajan a través del enlace troncal, las decisiones de envío se tornan más lentas y más difíciles de administrar, esto debido a que las tablas de conmutación de mayor tamaño tardan más en procesarse.

Los protocolos de enlace troncal se desarrollaron para administrar la transferencia de tramas de distintas VLAN, en una sola línea física de forma eficaz. Los protocolos de enlace troncal establecen un acuerdo para la distribución de tramas a los puertos asociados en ambos extremos del enlace troncal.

Modo	Función
Switchport mode access	Este modo ajusta la interfaz para que permanezca fuera del modo trocal (puerto de acceso). La interfaz permanecerá en este estado, aun cuando las demás interfaces se encuentren en el modo troncal.
Switchport mode dynamic desirable	Cualquier interfaz configurada en este modo intentara convertir su conexión a un enlace troncal. La interfaz permanecerá como un enlace troncal si las demás interfaces son ajustadas al modo *trunk, desirable o auto*. El modo determinado para todas la interfaces ethernet del switch es **dynamic desirable.**
Switchport mode dynamic auto	Hace que la interfaz sea capaz de convertir su conexión a un enlace troncal. En este modo, si las demás interfaces son configuradas al modo *trunk* o *desirable,* la interfaz permanecerá como un enlace troncal
Switchport mode trunk	Ajusta permanentemente la interfaz al modo de troncal y establece negociaciones para convertir la conexión a un enlace troncal. Si la interfaz se ajusta a este modo, permanecerá como un enlace troncal aún cuando las demás interfaces no estén configuradas como troncales.
Switchport nonegotiate	Evita que la interfaz generé tramas DTP, puede utilizar este comando solo cuando el modo de la interfaz sea de **acceso** o **trocal**. En este modo, debe configurar manualmente las demás interfaces como troncales para establecer un enlace troncal.

Tabla 5.1 Modos soportados por VTP

Los dos tipos de mecanismos de enlace troncal que existen son el filtrado de tramas y el etiquetado e tramas. El IEEE adopto el etiquetado de tramas como el mecanismo estándar del enlace troncal. Los protocolos de enlace troncal que usan etiquetado de tramas logran un envío de tramas más veloz y facilitan la administración. Los dos esquemas de etiquetado más comunes para los segmentos Ethernet son ISL y 802.Q.

5.2 El estándar 802.1Q

El estándar 802.1Q impone las siguientes limitaciones en la estrategia de trunking para una red.

1. En una red de switches Cisco conectados a través del estándar 802.1Q, los switches mantienen un Spaning Tree para cada VLAN permitida sobre el enlace troncal. Los equipos de otros fabricantes pueden soportar un STP para todas las VLANs. Cuando conecta un switch Cisco a otro switch de diferente fabricante a través de dicho estándar, el swith Cisco combinará el STP de la VLAN en el enlace troncal con el Spaning Tree del otro equipo. Sin embargo, la información de STP para cada VLAN se mantendrá separada en ambos equipos, los switch Cisco forman una nube (virtual) separada de los demás equipos.

2. Al utilizar este método de enlace troncal, debe asegurarse que la VLAN natural sea la misma en ambos extremos de la conexión. De lo contrario STP puede generar bucles y ocasionar problemas en la red.

3. Si en una conexión troncal, STP es deshabilitado solo en la VLAN natural y no en cada VLAN de la red, es muy probable que se generen bucles. Para evitar este problema, mantenga Spaning Tree habilitado en la VLAN natural o deshabilítelo en cada VLAN de la red. De esta manera, la red se encontrará libre de bucles.

La finalidad de un puerto troncal es enviar y recibir avisos VTP, para que pueda utilizar este protocolo, verifique que al menos un puerto del switch se encuentre configurado como un enlace troncal, y que a su vez, este puerto esté conectado a otro puerto (configurado como troncal) de un

segundo switch. De lo contrario, el switch no podrá enviar y recibir avisos VTP.

Antes de configurar una interfaz Ethernet como puerto troncal, debe considerar lo siguiente:

1. Un puerto troncal puede no ser un puerto seguro.

2. Un puerto troncal puede estar agrupado en **canales ethernet**, pero todos los troncales en el mismo grupo deben de tener la misma configuración. Si ha creado un primer grupo, los puertos restantes deben ajustarse con las mismas características de este grupo. Si modifica la configuración de uno de estos parámetros, tales como lista de permisos, prioridad de puerto para cada VLAN, velocidad del puerto y estado del enlace troncal, los cambios serán propagados hacia todos los puertos del grupo,

3. Si intenta configurar el estándar 802.1X sobre un puerto troncal, aparecerá un mensaje de error y el estándar no será habilitado.

4. Un puerto en modo dinámico puede negociar con su vecindario para convertirse en un puerto troncal. Si intenta habilitar 802.1X sobre un puerto dinámico, el sistema arrojará un mensaje de error debido a que esta membresía no es soportada por dicho estándar.

5. Puede implementar diversas medidas de seguridad sobre un puerto troncal.

5.3 Configuración de una interfaz Ethernet como un puerto troncal

Para configurar un puerto del switch como enlace troncal de acuerdo al estándar 802.1Q, siga los pasos que se describen a continuación:

1. Ubíquese en el modo privilegiado, después ingrese al modo de configuración global.

2. Acceda al modo de configuración de interfaz, esto le permitirá seleccionar el puerto que configurará como enlace troncal.

3. Después de seleccionar la interfaz correcta, ésta debe configurarse como un puerto troncal de capa 2, la figura 5.1 muestra como se realiza este proceso. Las opciones de configuración son las siguientes:

    - **Dynamic auto**. Este modo permite ajustar la interfaz a una conexión troncal si las demás interfaces se encuentran configuradas al modo trunk o al modo desirable.

    - **Dynamic desirable**. Modo que ajusta a la interfaz a una conexión troncal, siempre y cuando las demás interfaces están ajustadas al modo trunk, desirable o auto.

    - **Trunk.** El modo trunk ajusta la interfaz permanentemente al modo trunking. Realiza negociaciones para convertir la conexión a un enlace troncal cuando las demás interfaces no se encuentran en este modo.

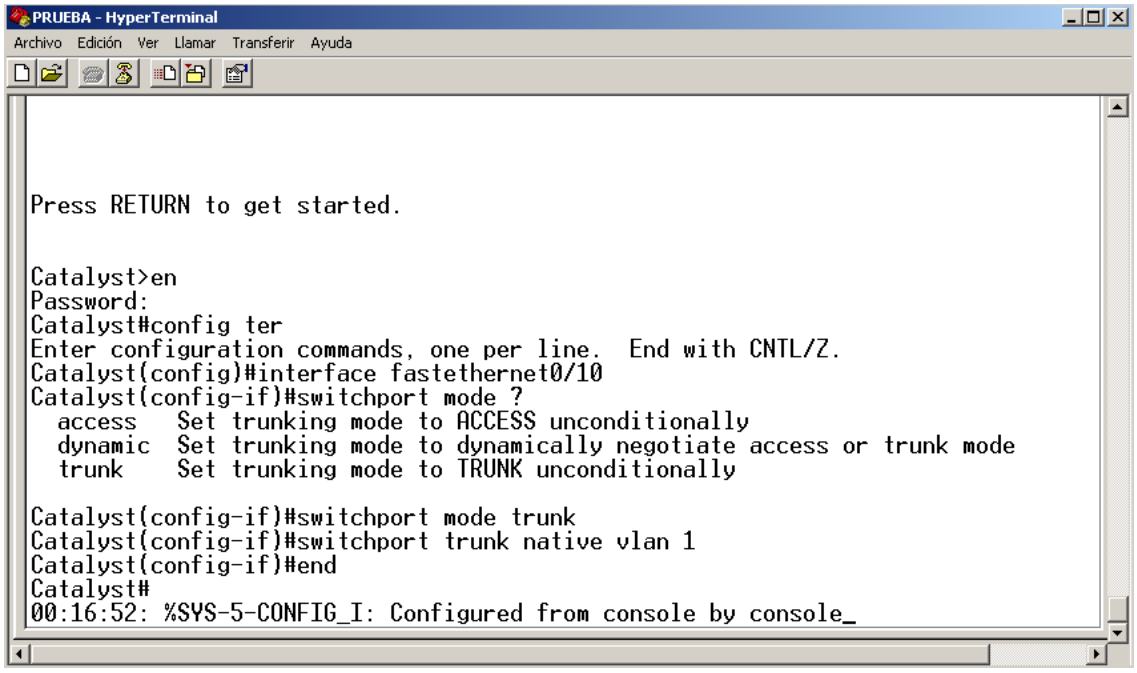

PRUEBA - HyperTerminal
Archivo Edición Ver Llamar Transferir Ayuda
Press RETURN to get started.
Catalyst>en
Password:
Catalyst#config ter
Enter configuration commands, one per line. End with CNTL/Z.
Catalyst(config)#interface fastethernet0/10
Catalyst(config-if)#switchport mode ?
access Set trunking mode to ACCESS unconditionally
dynamic Set trunking mode to dynamically negotiate access or trunk mode
trunk Set trunking mode to TRUNK unconditionally
Catalyst(config-if)#switchport mode trunk
Catalyst(config-if)#switchport trunk native vlan 1
Catalyst(config-if)#end
Catalyst#
00:16:52: %SYS-5-CONFIG_I: Configured from console by console_

Figura 5.1 Configuración de una interfaz como puerto troncal

4. Debe especificar la VLAN natural, para realizar esta acción utilice el comando **switchport trunk native vlan** *vlan-id.*

5. Después de realizar los ajustes adecuados, no olvide regresar al modo privilegiado, de esta manera la configuración tomará efecto.

6. Verifique la configuración de la interfaz. Las figuras 5.2 y 5.3 muestran el resultado de los comandos **show vlan y show interfaces** *interface-id* **switchport**. Después de comprobar que la configuración en la interfaz es la correcta, guarde los cambios en el archivo de configuración.

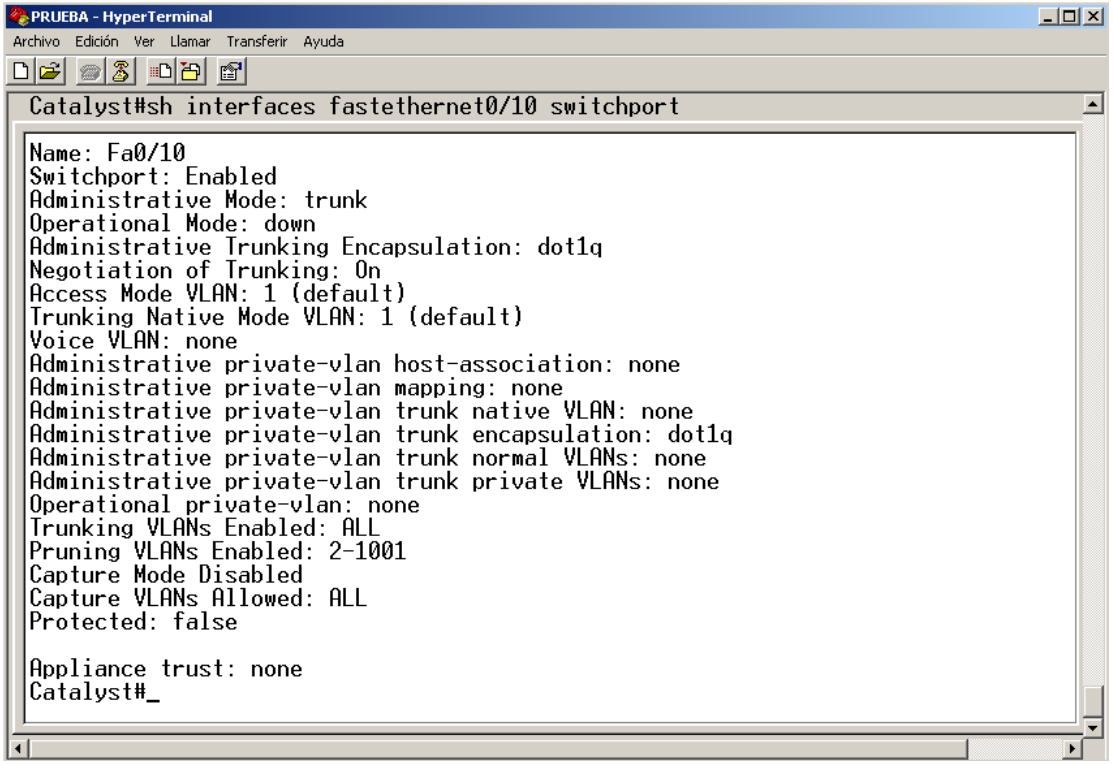


Figura 5.2 Resultado del comando **show interfaces** *interface-id* switchport después de configurar un puerto troncal

Si desea cambiar las características de la interfaz que ha configurado como enlace troncal, puede emplear alguno de los comandos listados en la tabla 5.2.

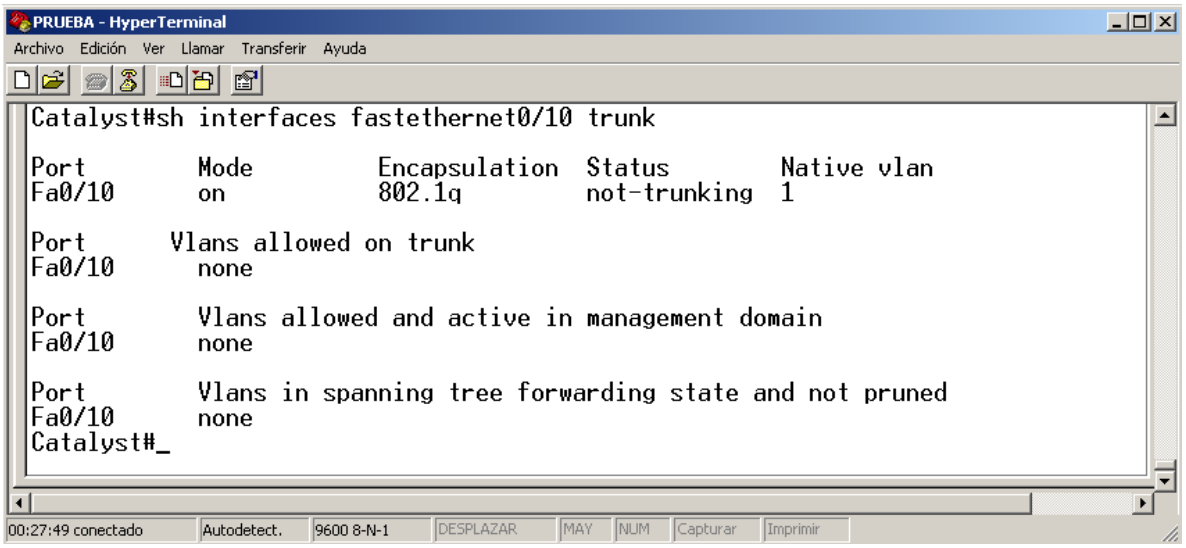


Figura 5.3 Resultado del comando **show interfaces** inteface-id **trunk** después de configurar un puerto troncal

Comando	**Descripción**
Defaul interface *interface-id*	Regresa la interfaz a su configuración defecto.
No switchport trunk	Reajusta todas las características del trunking a su estado predeterminado.
Switchport mode access	Permite configurar el puerto al modo de acceso estático.

Tabla 5.2 Con estos comandos la interfaz regresa a su configuración predeterminada.

Preguntas de repaso

43. Explique que es un enlace troncal.
44. Describa los modos de enlace troncal que pueden ser configurados en una interfaz.
45. Explique cual es la función del Protocolo Dinámico de Enlace troncal.
46. Explique las diferencias entre el etiquetado IEEE e ISL.
47. Describa la función de cada uno de los modos de configuración de interfaz al utilizar el estándar de etiquetado 802.1 Q.
48. Diga cuales son los modos validos cuando un puerto del switch es utilizado como enlace troncal hacia otro switch.
49. Diga cuales son los comandos utilizados para configurar un puerto de un switch como enlace troncal.
50. Describa el modo VTP que permite intercambiar la información VLAN entre switches.
51. Diga que tipo de interfaz debe utilizar si desea configurar un enlace troncal entre un switch y un router.

Práctica 5.1 Creación de un enlace troncal entre dos switches

Entre las ventajas que ofrece la segmentación VLAN se encuentra el control de broadcast y la seguridad, estas dos ventajas fueron parte del propósito de la practica 4.1, en la cual comprobó (en caso de que los resultados hayan sido los correctos) como esta tecnología incrementa la seguridad de la red.

Configurar VLANs en un switch que no se encuentra conectado a otros switches o routers en una red LAN o WAN puede no ser de gran utilidad, ya que las redes datos actuales de se encuentran interconectadas por cantidades considerables de equipos de comunicaciones.

En esta práctica realizará la configuración de un enlace troncal entre dos switches Cisco de la serie 2950, como recordará, estos equipos solo soportan el etiquetado de trama 802.1 Q.

1. Construya una red como se muestra en la figura 5.4

2. Seleccione una dirección IP (clase A, B, o C) y divídala en subredes. Si desconoce este proceso, puede utilizar las direcciones IP descritas en la tabla 5.3. En la cual se ha divido la dirección 192.168.10.0 en subredes de acuerdo a la mascara 255.255.255.224 (/27).

3. Configure la dirección IP y el default gateway en cada switch y host. Las direcciones seleccionadas deben estar en la misma subred. Haga ping a cada dirección IP; de host a host, de host a switch y de switch a switch. Asegúrese que éstos sean satisfactorios y anote los resultados en la tabla 5.4.

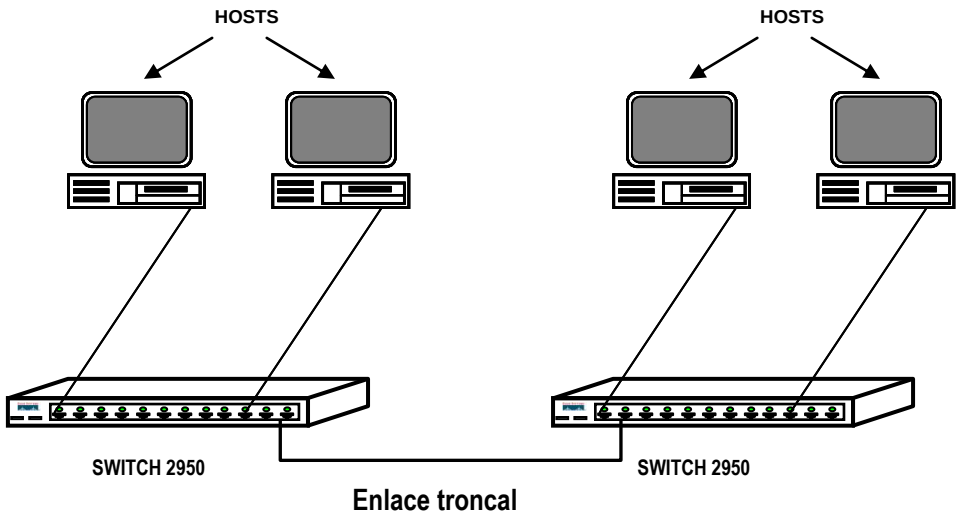


Figura 5.4 Configuración de un enlace troncal

Dirección de subred	Dirección de broadcast	Rango de direcciones
192.168.10.0	192.168.10.31	192.168.10.1 - 192.168.10.30
192.168.10.32	192.168.10.63	192.168.10.33 - 192.168.10.62
192.168.10.64	192.168.10.95	192.168.10.65 - 192.168.10.94
192.168.10.96	192.168.10.127	192.168.10.97 - 192.168.10.126
192.168.10.128	192.168.10.159	192.168.10.129 - 192.168.10.158
192.168.10.160	192.168.10.191	192.168.10.161 - 192.168.10.190
192.168.10.192	192.168.10.223	192.168.10.193 - 192.168.10.222
192.168.10.224	192.168.10.255	192.168.10.225 - 192.168.10.254

Tabla 5.3 División en subredes de la dirección 192.168.10.0

4. Seleccione una interfaz en cada switch y de acuerdo al procedimiento descrito en la sección 5.3, configúrela como un enlace troncal tal como lo muestra la figura 5.4 (no olvide que el cable que conectará a ambos equipos debe ser un cable cruzado). Utilice el comando **show vlan** para verificar la membresía de los puertos seleccionados en ambos switches.
5. En el switch A, configure VTP al modo cliente (el cual debe ser el modo predeterminado del switch). Cree dos VLANs y asígneles por lo menos dos interfaces diferentes al puerto seleccionado como enlace troncal.

6. Configure VTP en el switch B al modo cliente, después, verifique que este switch haya recibido los avisos procedentes del switch A. Para ello utilice el comando **show vlan brief,** el cual deberá mostrar en pantalla las VLANs (con sus respectivos identificadores) que fueron creadas en el otro switch.

7. Después de comprobar que las VLANs se encuentren en el switch B, asigne dos interfaces a cada una, recuerde que éstas deberán ser diferentes a la interfaz configurada como troncal.

8. Conecte un host en alguna interfaz del switch A designada a una VLAN. En el switch B, conecte otro host en otra interfaz asignada a la misma VLAN a la que conectó el host en el switch A. Configure nuevamente cada host con una dirección IP, ambas direcciones deben ubicarse en la misma subred.

Host	Dirección IP	Resultado de ping
Switch A		
Switch B		
PC 1		
PC 2		
PC 3		
PC 4		

Tabla 5.4 Configure cada host con una dirección IP

Las subredes y los rangos disponibles se indican en la tabla 5.3 (puede utilizar cualquier tipo de dirección IP, siempre y cuando, pueda dividirla en una cantidad de subredes adecuada al ejemplo). Posteriormente, utilice el comando ping para verificar la conexión entre ambos host y el swith. Los resultados de las pruebas de conexión deben ser satisfactorios ya que los host se encuentran en la misma VLAN.

9. Después de realizar correctamente las acciones establecidas en el punto anterior, y obtener los resultados indicados. Ahora, cambie de puerto el host en el switch B, conéctelo en algún puerto asociado a una VLAN diferente a la que conecto su igual en el switch A. Mediante el comando ping verifique la conexión entre ambos host, los resultados de las pruebas de conexión deben ser insatisfactorias, ya que los hosts se encuentran en VLANs diferentes.

10. Puede utilizar la tabla 5.5 para registrar los resultados obtenidos.

VLAN	Host	Puertos asignados
1		

Tabla 5.5 Registre los resultados obtenidos.

CAPITULO

VI

APORTACIONES

6.1 Aportaciones

Realizar la configuración de VLANs puede resultar una labor muy sencilla o complicada, un factor de suma importancia en el aprendizaje del funcionamiento y configuración de cualquier tecnología de conmutación, es la fuente didáctica utilizada para su estudio teórico y practico.

Las herramientas de estudio no solo deben poseer una estructura que cubra todos, o la mayoría de los aspectos relacionados con el tema que describen, si no que deben ser capaces de satisfacer las necesidades de quien las consulte.

Como se menciona en el capitulo uno, este trabajo práctico:

1. Proporciona la información necesaria para que el lector conozca y describa el funcionamiento de esta tecnología.

2. Proporciona al lector los conocimientos prácticos para implementar redes de área local virtuales.

Para lograrlo, se realiza la integración del ambiente teórico y practico. Generalmente, las guías de configuración proporcionadas por los fabricantes, están limitadas a describir el proceso de configuración y no incluyen información que describa el funcionamiento de la tecnología incorporada en sus equipos.

Cuando se logra la comprensión del funcionamiento de esta técnica de conmutación, resulta más fácil entender los resultados obtenidos al ingresar los comandos relacionados con dicho proceso de configuración. Inclusive, pueden interpretarse resultados inesperados que indiquen errores en tal proceso.

Para superar las deficiencias descritas con anterioridad, este trabajo ha sido elaborado de tal manera que proporciona en sus primeros capítulos, la información que permite comprender no solamente el funcionamiento de esta tecnología, si no que además, presenta un capítulo dedicado a explicar las herramientas lógicas en las cuales el switch basa su funcionamiento.

Además, para no perder el sentido practico del tema, se presentan los resultados obtenidos en la interfaz de configuración de cada uno de los comandos utilizados en cada proceso de configuración descrito. De tal manera que el lector se familiarice con el equipo y se prepare para los ejercicios prácticos.

6.2 Conclusiones

Los servicios de voz, datos y video basados en la tecnología VLAN, ofrecen el potencial que permite a las organizaciones que prestan ó adquieren servicios de telecomunicaciones, gestionar los cambios relacionados con el desarrollo tecnológico de la estructura de la red.

La implementación de VLANs permite resolver muchos problemas que suelen presentarse en una red, justificando de está manera la inversión económica que representa. Cualquier organización que invierta recursos considerables relacionados con movimientos de equipos o personal, puede justificar la incorporación de está tecnología.

El sector de las comunicaciones se vuelve cada vez más un entorno sumamente complejo, esto debido a la convergencia y el desarrollo tecnológico de los servicios de vos, datos y video. Por lo anterior, conocer el funcionamiento y configuración no solo de está tecnología, resulta de vital importancia en la formación de profesionales que pretendan desarrollarse en el sector de las telecomunicaciones.

ANEXO

A

REFERENCIA DE COMANDOS

Este anexo proporciona un resumen de todos los comandos del IOS de Cisco vistos a lo largo de este trabajo. Los comandos se distribuyen en tablas; cada tabla contiene un listado de comandos asociados, los cuales se presentan por orden alfabético en cada una de las tablas.

Puesto que algunos comandos coinciden parcialmente, es posible que encuentre variaciones del mismo comando en más de una tabla, pero el hecho de que los comandos estén agrupados por su respectivo uso y función, debe aclarar cualquier duda respecto a un grupo de comandos seleccionados. Además, se da por supuesto, que cada comando se ejecuta introduciéndolo el modo indicado en cada tabla.

Comandos de análisis

Los comandos de análisis permiten consultar rápidamente el estado de las interfaces del switch y otros parámetros asociados. La tabla A.1 resume estos comandos.

Comando	Descripción
Show vlan	Utilice este comando para visualizar la configuración de los parámetros relacionados con todas las VLANs creadas en el switch, tales como: nombre, identificador, puertos asignados, estado, tipo, tamaño de la MTU, etc. Para consultar los parámetros relacionados con una VLAN en particular, escriba el nombre o número de identificador asignado a dicha VLAN.
Show vlan brief	Muestra el nombre, estado y los puertos asignados a cada VLAN configurada en el switch.
Switchport acces	Comando de configuración de interfaz que permite configurar una interfaz como un puerto de acceso estático o dinámico. Si el modo es estático, la interfaz deberá ser asociada manualmente con alguna VLAN, si el modo es dinámico, la interfaz determinará su membresía en base a los paquetes que reciba.

Tabla A.1 Comandos de análisis

Comando	Descripción
Switchport acces	Para restablecer la interfaz al modo predeterminado, utilice la forma no de este comando.
Switchport mode	Utilice este comando en el modo de configuración de interfaz para definir el tipo de membresía VLAN que será asociada a una interfaz del switch, el modo puede ser: • access. Puerto de acceso estático • desirable. Realiza negociaciones con otras interfaces para configurar un puerto troncal • trunk. Ajusta la interfaz como un puerto troncal
Show interfaces	En el modo privilegiado, muestra el estado operacional y administrativo de todas las interfaces. Para consultar el estado de una interfaz en particular, escriba el nombre de dicha interfaz.
Show interfaces switchport	Muestra el estado administrativo y operacional de las interfaces que están conmutando paquetes.
Show running-config vlan	Muestra la configuración de todas las VLANs creadas en el switch.
Show startup-config	Comando del modo privilegiado que muestra la configuración del switch almacenada en la memoria NVRAM y es utilizada cuando este es reiniciado.
Show running-config	Comando del modo privilegiado que muestra la configuración del switch que se está ejecutando en la RAM.
show version	Muestra la versión del IOS que se está ejecutando en el switch.
Show history	Muestra un listado con los 10 últimos comandos utilizados

Tabla A.1 Comandos de análisis (continuación)

Comandos de configuración de nombre y contraseña

La tabla A.2 muestra los comandos que permiten cambiar las distintitas contraseñas incluidas en el switch, tales como la contraseña de conexión y la contraseña secreta de activación del modo privilegiado.

Comando	Descripción
Enable secret password [*contraseña*]	Comando de configuración global que permite cambiar en el switch la contraseña del modo privilegiado.
Hostname [*nombre*]	Comando de configuración global que permite cambiar el nombre del switch.
Line console 0	Permite lanzar el modo de configuración de línea para determinar la contraseña del switch.
Line vty 0 4	Permite lanzar el modo de configuración de terminal virtual para establecer la contraseña del teminal virtual.
Password [*contraseña*]	Se utiliza en los modos de configuración de línea y terminal virtual para determinar la contraseña de acceso a estos modos del switch.
enable	Permite ingresar al modo privilegiado
Banner motd	Comando de configuración global que permite crear una portada para la pantalla de conexión al switch.

Tabla A.2 Comandos de ajuste de nombre y contraseñas

Comandos de configuración

Como su propio nombre lo indica, estos comandos se refieren a la configuración de las interfaces incluidas en el switch; físicas y virtuales, La tabla A.3 muestra un resumen de los comandos de configuración utilizados.

Comando	Descripción
Configure terminal	Comando del modo privilegiado que permite lanzar el modo de configuración de interfaz.
Ctrl+C	Aunque no se trata de un comando de interfaz, se utiliza para cerrar una sesión de configuración.
encapsulation	Comando de configuración de interfaz especifico que permite determinar el tipo de encapsulación para una interfaz FastEthernet, GigabitEthernet o serial de un router.
interface	Comando de configuración global utilizado para configurar una interfaz (FastEthernet o GigabitEthernet), crear una interfaz virtual para ser usada como la interfaz de administración VLAN, y acceder al modo de configuración de interfaz.
vlan	Este comando puede ser utilizado en dos modos diferentes de configuración. • Modo de configuración global.Utilice este comando para crear o modificar un VLAN. Para eliminar una VLAN utilice la forma no de este comando. • VLAN configuration. Para ingresar a este modo debe utilizar el comando vlan database en el modo privilegiado, y utilizar el comando vlan para crear VLANs en el rango normal.
Vlan database	Utilice este comando en el modo privilegiado para ingresar al modo VLAN configuration, en el cual podrá crear, modificar y eliminar VLANs en el rango normal. La configuración realizada será guardada en la base de datos VLAN.
Ip address	Comando de configuración de interfaz que permite configurar una dirección ip en el switch para propósitos de administración remota. Después de introducir el comando ip address, escriba la dirección IP asignada y la máscara de subred de dicha dirección. Para poder acceder al switch a través de esta dirección, al menos una interfaz debe estar asociada a la VLAN de administración.

Tabla A.3 Comandos de configuración

Comando	Descripción
shutdown	Comando de configuración de interfaz que permite deshabilitar un puerto, para bloquear la interfaz de administración VLAN, escriba el subcomando vlan después de comando shutdown. Para activar nuevamente una interfaz, ingrese la forma no de este comando.
vtp	Puede utilizar este comando en los modos siguientes: • Utilice el comando de configuración global vtp para modificar los parámetros de VTP. • Utilice el comando privilegiado EXEC para configurar el password, prunning y versión VTP. • Modificar los parámetros VTP en el modo config vlan.
Ping [*dirección IP*]	Comando utilizado para comprobar la conexión entre dos switchs, un switch y un router, dos PCs, o cualquier dispositivo configurado con alguna dirección IP, siempre y cuando soporte este comando.
rcommand	Comando utilizado para iniciar una sesión Telnet.
Copy running-config startup-config	Permite copiar en la memoria NVRAM la configuración que se está ejecutando.

Tabla A.3 Comandos de configuración (continuación))

ANEXO

B

CARACTERISTICAS DE LOS SWITCH CISCO SERIE 2950

Los switches Cisco Catalyst 2950SX-48, 2950T-48, 2950SX-24, 2950-24 y 2950-12 forman la serie 2950. Son switches independientes con un número determinado de puertos 10/100 Mbps, son ideales para la conexión de redes pequeñas y de tamaño mediano. Ésta serie incluye el Software Image estándar (SI) y ofrece todas las funcionalidades para el soporte de servicios de datos, voz y video.

Los switch catalyst 2950-12 y 2950-24 proporcionan una combinación de puertos 10/100 Mbps respectivamente. Si el diseño de la red incluye conexiones uplink en fibra óptica, puede elegir entre la serie 2950SX-24 que proporciona 24 puertos 100 Mbps y dos puertos 1000BASE-SX, y la serie 2950SX-48 que incluye 48 puertos 100 Mbps y dos puertos 1000BASE-SX. Los Catalyst 2950T-48 son switches que incluyen 48 puertos 10/100 Mbps dos puertos 10/100/1000 Mbps para conexiones a base de cobre y sirven como una solución alternativa al costo de la fibra.

Figura B.1 Switch Catalyst 2950-12

Figura B.2 Switch Catalyst 2950-24

Figura B.3 Switch Catalyst 2950SX-24

Figura B.4 Switch Catalyst 2950T-48

Figura B.5 Switch Catalyst 2950SX-48

Seguridad de la red

Los switchs Catalyst 2950 ofrecen seguridad de la información a través de un amplio rango de características de seguridad. Estas características permiten a los clientes proporcionar seguridad basada en los usuarios y en el direccionamiento MAC. La protección de la información se realiza mediante el protocolo SSHv2 (Secure Shell versión 2), el cual usa técnicas de cifrado que hacen que la información que viaja por la red vaya de manera no legible y ninguna otra persona pueda descubrir su contenido.

La configuración de VLANs aisla los puertos en el switch, asegurando que el tráfico viaje directamente desde el puerto de entrada a el dispositivo destino, a través de la trayectoria virtual y éste no pueda ser reenviado a otro

puerto. Para la autenticación de los usuarios con sistema de control de acceso a terminales (TACACS) en conjunto con un servidor RADIUS, el protocolo 802,1 x proporciona un alto nivel de seguridad ya que permite la autenticación dinámica de los usuarios basada en puerto. Este tipo de autenticación puede ampliarse dinámicamente para asignar una VLAN a algún usuario específico independientemente del lugar donde se conecte a la red.

Con las características de seguridad integradas en el switch Cisco Catalyst 2950, los puertos son altamente seguros. La seguridad de los puertos basada en el direccionamiento MAC previene que estaciones no autorizadas accedan al switch, a demás la seguridad de acceso multinivel en la consola del switch y en las interfaces de administración vía web evitan que usuarios no autorizados modifiquen la configuración del switch.

Control de la Red

Los switchs Catalyst 2950 proporcionan calidad deL servicio en etapas, soportando dos modos de reclasificación. Uno basado en el estándar IEEE 802.1p que hace referencia a la clase de servicio (class-of-service, CoS), el cual determina el punto de ingreso del paquete y lo asigna a la cola apropiada. En el segundo, el paquete puede ser clasificado en base al valor defecto del CoS asignado en el puerto de ingreso por el administrador. Para el caso de las tramas que son recibidas sin ningún valor CoS (tales como tramas no etiquetadas), los switch Catalyst 2950 realizan la clasificación basada en el valor CoS predeterminado por el administrador de la red.

Después que las tramas han sido clasificadas mediante alguno de los modos anteriormente descritos, estás son asignadas a la cola de salida apropiada. Los switch Cisco de la serie Catalyst 2950 soportan cuatro colas de salida, las cuales permiten al administrador ser más discriminante en la asignación de las prioridades para varias aplicaciones en la LAN.

La configuración de un esquema estricto de prioridad asegura que las aplicaciones sensibles a los retardos como la voz , sigan una trayectoria adecuada en la nube de switches.

Estas características permiten al administrador de la red dar prioridad a las aplicaciones sensibles al tiempo como lo es la telefonía IP, recursos de planeación empresariales (Oracle, SAP), diseño asistido por computadora o e-mail.

Disponibilidad de la red

Para efectuar el uso adecuado de los recursos de red como el ancho de banda, los switchs Cisco Catalyst soportan el Protocolo de Administración de Grupo de Internet versión 3 (IGMPv3), que en conjunto con la herramienta de gestión de redes Cisco Network Assistand permite el manejo y administración de aplicaciones multicast en una LAN.

Las características de IGMPv3 permiten al switch escuchar las conversaciones entre host y routers. Cuando un switch escucha una petición IGMP de un host hacia un grupo multicast, el switch añade el número del puerto del host a la lista de direcciones destino del grupo. Después, cuando recibe un mensaje dirigido a la dirección de grupo almacenada, lo enviará sólo por los puertos por donde haya escuchado mensajes de unión a ese grupo.

El protocolo Per VLAN Spanning Tree Plus (PVST+) permite a los usuarios implementar conexiones redundantes para distribuir el flujo de datos a través de múltiples enlaces. Esto no es posible con implementaciones estándar de STP, la tecnología Cisco UplinkFast asegura la transferencia inmediata por conexiones secundarias que proporcionan un tiempo de convergencia mejor que el tradicional de 30 ó segundos.

Administración de la red

El administrador puede configurar cada switch con el Cisco Device Manager, o si lo prefiere, configurar y resolver problemas relacionados con switches mediante el Cisco Network Assistant, el cual es un software de administración de redes ideal para aplicarse en LAN pequeñas y empresas de tamaño medio de hasta 250 usuarios.

Cisco Device Manager ofrece una interfaz simple para configurar y monitorear el switch, con esta herramienta los usuarios tienen la opción de ajustar el switch vía web. De esta manera se elimina la necesidad de utilizar programas de emulación de terminal y evita el uso de la interfaz de línea de comandos.

Con el asistente para red de Cisco, el administrador de la red puede configurar múltiples puertos y switchs simultáneamente. Los gráficos de ancho de banda, los reportes de conexión y la topología de la red proporcionan al administrador una visión rápida del estado de la red.

El ayudante Cisco AVVID (Architecture for Voice, Video and Integrated Data) proporciona configuración automática del switch para optimizar el soporte de aplicaciones de video, voz sobre IP y otras aplicaciones criticas.

Adicionalmente, los switch Catalyst 2950 proporcionan una herramienta de administración de red basada en el protocolo SNMP, con esta herramienta los switchs pueden ser configurados y administrados en base al tipo de dispositivo conectado al puerto, VLAN, tipo de tráfico y a las políticas de manejo. Las tablas siguientes describen las características de softaware y hardware, a si como también, los beneficios proporcionados por las series de switchs Cisco Catalyst 2950.

Característica	Protocolos soportados
Seguridad	• Soporte de VLANs • Autentificación de acuerdo al estándar 802.1x (telefonia IP y seguridad del puerto) • Encriptación de los datos durante sesiones Telnet de acuerdo al Protocolo SSHv2 • Seguridad del puerto basada en el direccionamiento MAC • Autentificación mediante servidores TACACS y RADIUS • Soporte de sistema de detección de intrusos SPAN • Monitoreo, control, administración mediante el protocolo SNMP • Cisco Network Assistant
Calidad de servicio (QoS de Capa 2)	• Reclasificación de tramas de acuerdo al estandár 802.1p class of service (CoS) • Soporte de algoritmos Weighted Round Robin (WRR) • Manejo de 4 colas con prioridad por cada puerto para implementar CoS (802.1p)
Administración	• Administración y configuración por medio de sesiones Telnet o a través de la CLI • Soporte RMON, grupos de Alarmas, Eventos, Estadísticas, e Historia
Administración	• Soporte de Network Timing Protocol (NTP) y Trivial File Transfer Protocol • LEDs indicadores de estado de los puertos • Soporte de Response Time Monotoring (RTTMON) • Soporte de STP y PVST • Soporte de Remote Switch Port Analyzer (RSPAN) y Switch Port Analyzer local.
Herramientas de Cisco Works	• Soporte de SNMP versión 1 y2 para encriptación de sesiones (Telnet y CLI) • Soporte de Cisco Discovery Protocol (CDP) versión 1 y 2.

Tabla A.1 Especificaciones de Software

Característica	Protocolos soportados
Facilidad de empleo y despliegue	• Cisco Device Manager • Cisco Express Setup • Cisco VTP • Soporte de Link Aggregation Control Prorocol LACP (estándar IEEE 802.3 ad) • Soporte de VLAN Membership Policy Server (VMPS) • Auto-negociación en todos los puertos • Función de auto-detección en cada puerto • Auto-configuración a través de servidores BOOTP • Asignación dinámica de VLAN

Tabla A.1 Especificaciones de Software (Continuación)

Característica	Descripción
Construcción	• Switching fabric de 8.6 Gbps • 4.8 Gbps de maximum forwarding bandwidth • 3.6 Mbps de wire speed forwarding rate (basado en paquetes de 64 Bytes) • 8 MB de memoria compartida • 16 MB de memoria DRAM y 8 MB de memoria FLASH • 8000 direcciones MAC • LEDs incadores de estado • Dimensión y longitud: 1,72 x 17.5 x 9.52 in • Peso 6.5 lb
Conectores	• Puertos Ethernet 10/100 Base T con conector RJ-45 • Puerto de consola (conector RJ-45 a DB9) • Conector para fuente de energía • Conector para fuente redundante de energía (opcional)
Ambiente de operación	• Temperatura de operación: 0 - 45 °C • Temperatura de almacenaje: - 25 °C - 70 °C • Hemedad relativa: 10 – 80 % (sin condensación)

Tabla A.2. Especificaciones de Hardward

Característica	Descripción
Requerimientos de energía	• Consumo de energía: 30 W-102 BTUs/hr, máximo 45 W – 154 BTUs/hr • Voltaje de entrada: 100-127 VCA, 200-240 VCA • Frecuencia de entrada: 47 a 63 HZ • Voltaje de entrada DC (para Cisco RPS 675 y RPS 300): +12 V 4.5 A
Certificaciones de Seguridad y emisión electromagnética	• UL 60950/CSA 22.2 No. 950 • IEC 60950/EN 60950 • AS/NZS 3260, TS001 • CE Parking • FCC Part 15 Class 5 • ENN 55022 • MIC • CNS 13438 Class A • AS/NZS 3548 Class A • VCCI Class A • CLEI Code

Tabla A.2. Especificaciones de Hardware (continuación)

ANEXO

C

DESCRIPCION DEL PROTROCOLO VTP

El VLAN Trunking Protocol (VTP) proporciona un medio sencillo para mantener una configuración de VLAN coherente a través de toda la red, ofrece soluciones de red conmutada fácilmente escalable, reduciendo la necesidad de configuración manual de la red. Mantiene una correlación de la configuración VLAN a través de un dominio de administración común, gestionando las adiciones, supresiones y cambios de nombre en las VLAN a través de la red.

VTP es un protocolo de intercambio de mensajes de capa 2, el cual mantiene una configuración consistente para administrar la adición, eliminación y renombre de las VLANs en una red. VTP minimiza el trabajo de configuración que puede causar problemas como nombres duplicados, especificaciones incorrectas y violaciones de seguridad.

Antes de configurar una VLAN, debe decidir si va a utilizar VTP en la red. Con la ayuda de VTP, puede centralizar los cambios de configuración sobre uno o más switch. Estos cambios son enviados de manera automática a otros switch en la red. Sin VTP, no podrá intercambiar información VLAN con otros switchs.

VTP solo reconoce VLAN configuradas en el rango normal, el rango extendido no es soportado por VTP, no es almacenado en la base de datos VLAN y es soportado cuando el EI esta instalado en el switch.

El dominio VTP

El dominio VTP, también llamado dominio de administración VLAN, consiste de uno o varios switch bajo una misma responsabilidad administrativa, los cuales comparten el mismo nombre de dominio VTP. Un switch puede ser su único dominio VTP, puede cambiar la configuración global VLAN del dominio

a través de la CLI, o si lo prefiere, puede utilizar el protocolo simple de administración de red (SNMP).

Por defecto, el switch se encuentra en el estado de dominio no administrativo, permanecerá en este estado hasta que reciba un aviso sobre un enlace troncal o hasta que configure el nombre de dominio al que pertenecerá. Hasta entonces no podrá crear o modificar VLANs sobre un servidor VTP y por lo tanto la información no será propagada por la red.

Si el switch recibe un aviso VTP a través de un enlace troncal, éste obtendrá el nombre de dominio administrativo y revisará la configuración VTP. El switch ignorará los avisos que tengan un nombre de dominio diferente o cuenten con un número de revisión de mayor prioridad.

Antes de añadir un switch a un dominio VTP, verifique que su número de revisión sea menor que el número de revisión de otros switch. Los switches configurados en un dominio VTP, usarán siempre la configuración VLAN del switch que cuente con el número de revisión mayor. Si añade un switch que tenga un número de revisión mayor que el número de revisión del dominio VTP, éste puede borrar toda la información VLAN del servidor y dominio VTP.

Cuando realice un cambio en la configuración VLAN de un servidor VTP, el cambio es propagado a todos los switches en el dominio. Los avisos VTP son enviados sobre todas las conexiones troncales, VTP mapea VLANs de manera dinámica con un nombre único asociado, el mapeo elimina la administración excesiva de los dispositivos y facilita la labor del administrador de la red.

Modos VTP

Puede configurar un switch para que soporte alguno de los modos listados a continuación.

1. **Modo Servidor**. El modo VTP predeterminado es el modo servidor. En el modo servidor puede crear, modificar, eliminar y modificar otros parámetros que afectan todo el dominio VTP. Los servidores VTP envían su configuración VLAN a otros switches del mismo dominio y sincronizan sus configuraciones con otros switches en base a los avisos recibidos por los enlaces troncales. En modo servidor la configuración VLAN se guarda en la NVRAM.

2. **Modo Cliente**. Un switch que opere en el modo cliente no podrá crear, cambiar o suprimir VLANs. Un cliente VTP no guarda la configuración VLAN en memoria no volátil. Tanto en el modo cliente como en el modo servidor, los switches sincronizan su configuración VLAN con aquella que tenga el número de revisión más alto en el dominio VTP.

3. **Modo transparente.** Un switch que opera en este modo no genera avisos VTP y no sincronizará su configuración VLAN con la información recibida desde otros switchwes. Además, podrá crear, suprimir y modificar VLANs, pero los cambios no serán propagados a otros switchs y afectarán solo al switch local.

Los switches en modo transparente envían publicaciones VTP, pero ignoran la información que contiene el mensaje. Un switch transparente no modifica su base de datos cuando recibe alguna actualización, no obstante, envíara una actualización indicando que se ha producido un cambio en el estado de la VLAN.

Sin embargo, con la versión 2 de VTP, los switches que operen en el modo transparente difundiran los avisos VTP que reciban de otros switches. Al configurar VTP es importante elegir el modo adecuado, ya que VTP es una herramienta muy potente y puede crear problemas en la red.

Cuando el switch esta en modo transparente las configuraciones VTP y VLAN son almacenadas en la NVRAM, pero estas no son enviadas a otros switches.

Cuando se excede el número máximo de VLANs soportadas por el switch, éste cambiará automáticamente del modo servidor al modo cliente o transparente, la tabla C.1 muestra un resumen de las características de cada modo.

Modo VTP	Características
Modo servidor	Envía y retransmite avisos VTP. Sincroniza la información de configuración de VLAN con otros switches. El switch Catalyst puede crear VLAN. El switch Catalyst puede modificar VLAN. El switch Catalyst puede suprimir VLAN.
Modo Cliente	Envía / retransmite avisos VTP. Sincroniza la información de configuración de VLAN con otros switches. Las configuraciones de VLAN no se guardan en la NVRAM. El switch Catalyst no puede crear VLAN. El switch Catalyst no puede suprimir VLAN. El switch Catalyst no puede modificar VLAN.
Modo Trasparente	Retransmite avisos VTP. No sincroniza la información de configuración de VLAN con otros switches. Las configuraciones de VLAN se guardan en la NVRAM. El switch Catalyst puede crear VLAN. El switch Catalyst puede modificar VLAN. El switch Catalyst puede suprimir VLAN.

Tabla C.1 Características de lo modos VTP

Avisos VTP

Cada switch que pertenezca a un dominio VTP, enviará periódicamente avisos del estado de la configuración a cada puerto por el que reciba direcciones multicast. Los switches vecinos reciben estos avisos y si es necesario actualizan sus configuraciones VLAN y VTP.

Los anuncios VTP distribuyen la información siguiente:

a) Nombre de dominio VTP
b) Número de revisión de configuración
c) Actualización de identidad y
d) Formato de trama
e) Cifrado MD5 de la configuración VLAN

Para cada configuración VLAN los anuncios VTP distribuyen la información siguiente:

a) VLAN IDs
b) Nombre de la VLAN
c) Tipo de VLAN
d) Estado de la VLAN
e) Información de configuración adicional especificada por el tipo de VLAN.

Los avisos VTP inundan los puertos destinos a través del dominio de administración cada 5 minutos y/o cuando haya un cambio en la configuración de las VLAN. El aviso contiene el número de revisión, recuerde que el número de revisión más alto indica la configuración más actual.

VTP Pruning

El VTP pruning es un sistema que permite a los switches añadir o eliminar dinámicamente VLANs sobre un enlace troncal, creando una red mucho más eficiente. Por defecto, una VLAN esta asociada a una conexión troncal.

Si un host en una VLAN envía un broadcast, éste será difundido por todos los puertos del enlace troncal y se transmitirá a todos los host pertenecientes a dicha VLAN. Sin embargo, según la topología de la red, es probable que haya switches que no contengan ningún puerto asociado a esta VLAN, y pese a esto, recibirán este mensaje de broadcast.

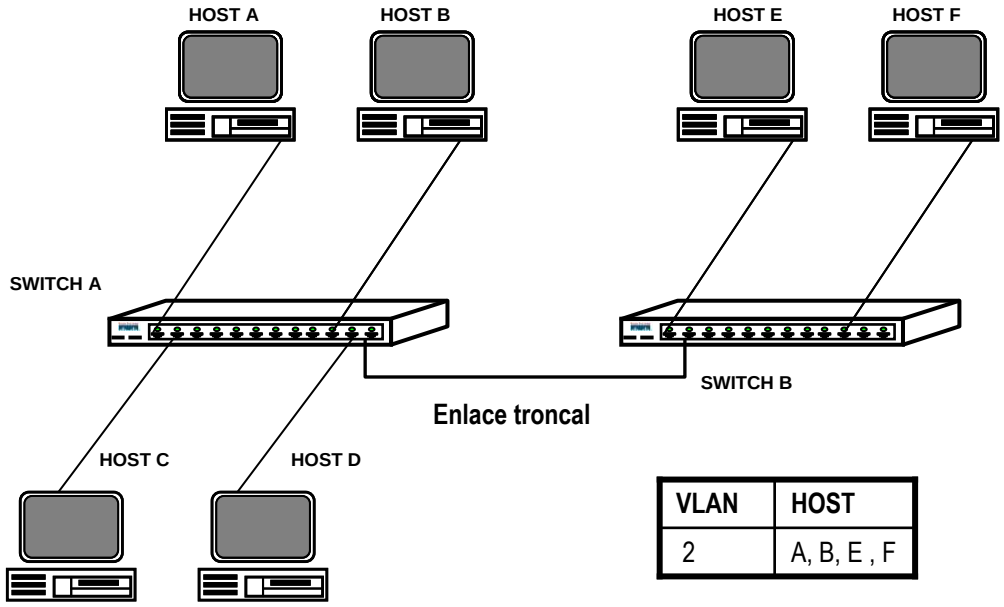


Figura C.1 Las difusiones broadcast disminuyen el rendimiento de la red

Considere la figura C.1, en la cual se supone que el pruning no está habilitado, los host A, B, E Y F se encuentran en la misma VLAN. Si el host A genera un broadcast, éste será recibido por el switch A, quien lo transmitirá al host B, y a través del enlace troncal que lo conecta con el switch B a los host E Y F.

Supongamos que el host C genera un broadcast el cual utiliza 10 Mb del ancho de banda disponible. El paquete es enviado al switch A, quien además de reenviarlo al host D, lo enviará al Switch B suponiendo que en este se encuentra algún host que lo recibirá.

Como puede observar, los dispositivos están utilizando innecesariamente la capacidad del enlace troncal, ya que al final, los paquetes enviados hacia el switch B serán descartados. Afortunadamente, existe un método para solucionar este problema; **el VTP pruning**.

El VTP pruning incrementa el ancho de banda disponible, ya que restringe el tráfico que inunda los enlaces troncales, que en la mayoria de los casos es utilizado para alcanzar dispositivos destino. Sin VTP pruning, un switch inundará la red con tráfico unicast, musticast y broadcast (innecesario) a través de todos los enlaces troncales dentro de un dominio VTP.

Los bloques VTP pruning no difunden paquetes (a través enlaces troncales) hacia VLANs que están incluidas en una lista reducible (pruning-eligible). Solamente las VLANs consideradas en esta lista podrán descartar este tipo de tramas. Por defecto, las VLANs 2 hasta 1001 se encuentran incluidas en ésta lista. El VTP prunning es soportado por ambas versiones de VTP (versión 1 y 2) y esta deshabilitado por defecto.

La figura C.2 muestra una red conmutada en la cual VTP pruning no esta habilitado. El puerto 1 en el switch 1 y el puerto 2 en el switch 4 están asignados a una VLAN. Si un broadcast es enviado desde el host conectado al switch 1, el switch 1 difundirá el broadcast y cada switch en la red lo recibirá, incluso los switch 3,5 y 6, los cuales no tienen puertos asignados a la red VLAN.

La figura C.3 muestra una red conmutada con VTP pruning habilitado. Los paquetes broadcast del switch 1 no son enviados hacia todos los switch

de la red, debido a que el tráfico por la red VLAN es reducido en los puertos 5 y 4 de los switchs 2 y 4.

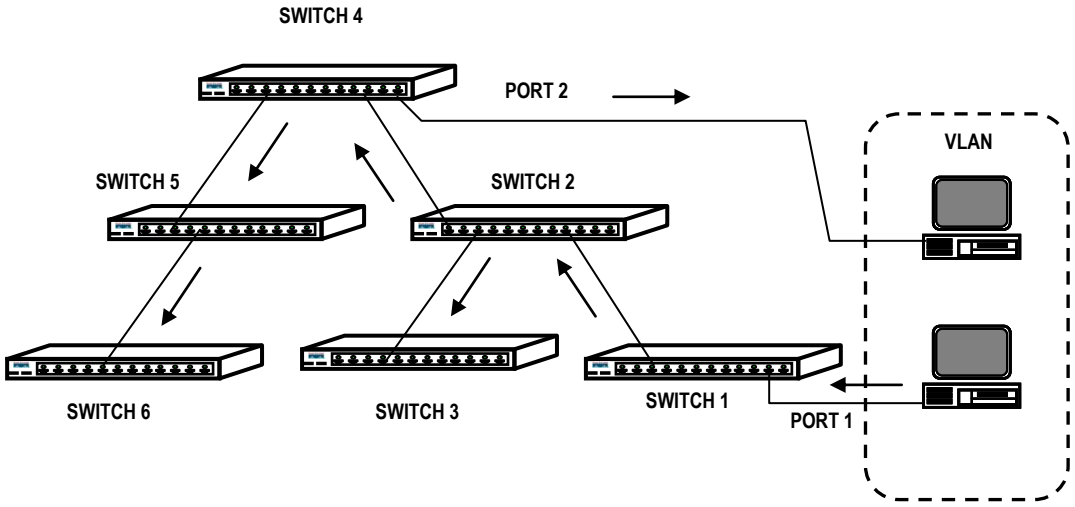


Figura C.2 Sin VTP pruning los broadcast se propagan por toda la red

Cuando activa el pruning en un switch configurado como servidor VTP, lo habilita para todo el dominio. VTP pruning no reduce el trafico de las VLANs que están en una lista no elegible (pruning ineligible). La VLAN 1, VLANs 2 a 1005, están siempre en esta lista, VTP pruning no esta diseñado para funcionar en el modo VTP transparente. Si uno o más switches se encuentran en este modo debe deshabilitar VTP pruning en toda la red.

Para configurar VTP pruning sobre una interfaz, use el comando de configuración de interfaz **switchport trunk pruning vlan.** La lista elegible de reducción (prunning-eligible) se aplica solamente a los puertos troncales. Cada puerto troncal posee una lista de elegibilidad, para que este proceso tenga efecto, VTP pruning debe ser habilitado, más adelante en este capítulo se describe el proceso empleado para realizar esta acción.

Configuración de VTP

Al igual que existen parámetros definidos para configurar VLANs, existen parámetros predeterminados para configurar VTP, estos parámetros se muestran en la tabla c.2.

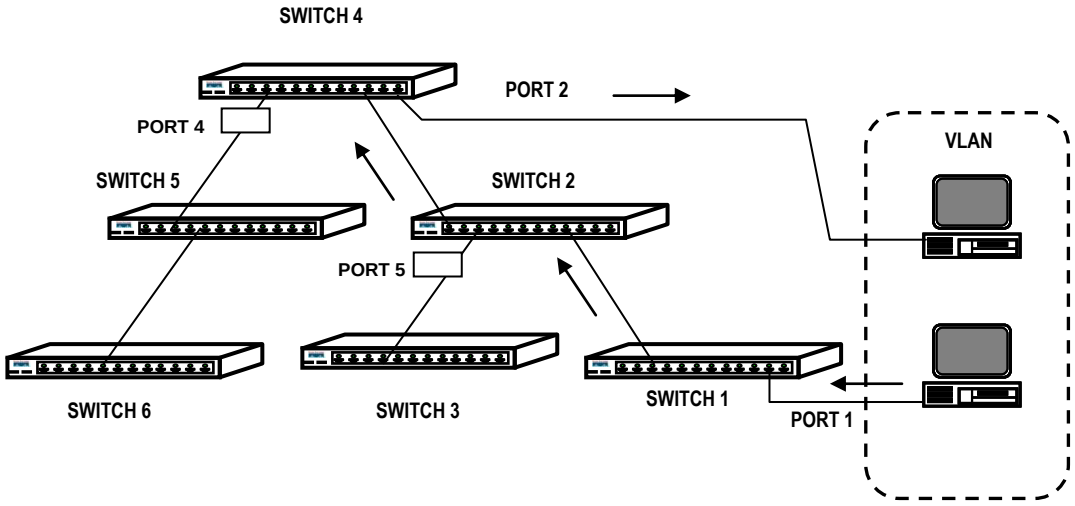


Figura C.3 El VTP pruning optimiza el desempeño de la red

Característica	Valor predeterminado
Nombre de dominio VTP	Nulo
Modo VTP	Servidor
Estado de VTP versión 2	Versión 2 deshabilitada
Contraseña para VTP	Ninguna
VTP Prunning	Deshabilitado

Tabla C.2 Configuración defecto para VTP

VTP en el modo de configuración global

Puede utilizar el comando **vtp** en el modo de configuración global para habiliar o deshabitar el prunning, configurar la contraseña, versión, nombre del archivo, interfaz de actualización, nombre de dominio y el modo de operación de VTP. Cuando VTP se encuentra en el modo transparente, el nombre de dominio y modo son guardados en el archivo de ejecución del switch, para guardar una copia en el archivo de arranque debe ingresar el comando **copy running-config startup-config** en el modo privilegiado. Utilice este comando para evitar que la configuración se pierda en caso de reiniciar el switch.

Cuando VTP se encuentra en modo transparente en el archivo de arranque del switch, la configuración del switch se determina de la manera siguiente:

1. Si en el archivo de arranque VTP se encuentra en el modo transparente y el nombre de dominio VTP es diferente tanto en este archivo como en la base de datos VLAN, el switch utilizará la configuración indicada en el archivo de arranque e ignorará la información contenida en la base de datos.

2. Si el modo VTP y el nombre de dominio son diferentes en el archivo de arranque y en la base de datos, el switch tomará la configuración de estos parámetros según se indique en la base de datos.

VTP en el modo vlan configuration

A diferencia del modo anterior, éste permite configurar todos los parámetros relacionados con VTP, para entrar a este modo, solo tiene que escribir la instrucción **vlan data base** en el indicador del modo privilegiado. Cuando ingrese el comando exit, los comandos utilizados en la configuración serán aplicados para actualizar la base de datos y los mensajes VTP serán enviados hacia los switches ubicados en el mismo dominio.

Si VTP esta en el modo transparente, el nombre de dominio será guardado en el archivo de ejecución. Para almacenar esta información en el archivo de arranque deberá utilizar el comando **copy running-config startup-config**.

Configuración de VTP en los modos servidor, cliente y transparente.

Para realizar cambios relacionados con la configuración VLAN, y que estos cambios sean propagados por toda red, debe ajustar VTP al modo servidor. Como se menciono en la sección anterior, dispone de dos métodos para realizar los ajustes de los parámetros VTP, cada uno posee características particulares, por lo que ambos serán descritos en esta sección.

Para configurar VTP en el modo global, realice el procedimiento que se describe a continuación:

1. En el indicador de modo privilegiado, ingrese el comando **configure terminal**, con esto entrará al modo global.

2. Para configurar VTP al modo servidor, escriba el comando vtp mode server. Deberá aparecer un mensaje indicándole que el switch se encuentra en este modo (si es que no fue cambiado con

anterioridad), ya que este es el modo predeterminado en todos los switchs Cisco.

3. Asigne un nombre de dominio, éste debe estar formado por un máximo de 32 caracteres. Todos los switchs que operen con VTP en el modo cliente o servidor y estén bajo una administración común, deben ser configurados con el mismo nombre de dominio. Los switches con VTP en el modo transparente, no intercambian mensajes entre ellos. Para configurar el nombre de dominio ingrese el comando **vtp domain** *domain-name*, donde las letras en cursivas representan el nombre seleccionado.

4. Puede configurar un password para el dominio VTP, sin embargo, no es requerido. En caso de hacerlo, debe ser el mismo en todos los switches que forman el dominio. Para ajustar el password, ingrese el comando **vtp password** *password*, debe tener 8 caracteres como mínimo y un máximo de 64.

5. Los switchs que carezcan de esta información o posean uno equivocado rechazaran los avisos procedentes de otros switches. Si añade otro switch (Cisco) a la red existente, en el cual VTP se encuentre deshabilitado, el nuevo switch aprenderá el nombre de dominio solo después de ajustar el password correcto.

6. Para regresar al modo privilegiado escriba el comando **end**, después con el comando **show vtp status** verifique los cambios realizados.

También puede utilizar el modo vlan configuration para ajustar los parámetros VTP; ubíquese en el modo privilegiado EXEC y realice el procedimiento que se describe a continuación:

1. Para ingresar al modo vlan configuration, escriba el comando vlan database

2. Ahora ajuste VTP al modo servidor escribiendo el comando **vtp verver**.

3. Mediante el comando vtp domain domain-name configure un nombre de dominio, al igual que en el método anterior debe utilizar 32 caracteres como máximo.

4. Con el comando **vtp password** *password* ajuste la contraseña para el dominio VTP, la cual debe tener 8 caracteres como mínimo y un máximo de 64.

5. Para actualizar la base de datos VLAN y que los ajustes realizados sean propagados a través del dominio, escriba el comando **exit**.

6. Con el comando **show vtp status** verifique los cambios realizados.

Para desactivar la contraseña en el switch, en el modo privilegiado escriba el comando **no vtp password**, sin importar que método utilizo para ajustarla.

Si revisa con detalle ambos métodos de configuración, observará que la única diferencia que existe entre ellos se encuentra en el paso 1, y consiste en el comando ingresado después de ubicarse en el modo privilegiado.

Para cambiar VTP al modo cliente, realice las mismas acciones descritas en ambos métodos de configuración; vlan configuration y vlan data

base. Solo que en el paso 3, deberá escribir en comando **vtp mode client** en lugar de **vtp mode server**.

Para deshabilitar VTP en el switch, debe ajustarlo al modo transparente. En este modo el switch no enviará actualizaciones VTP e ignorará las actualizaciones recibidas desde otros switches. Sin embargo, si configura VTP al modo transparente en un switch que este funcionando con VTPv2. Este switch enviará los avisos recibidos por los enlaces troncales a los que este conectado.

Para deshabilitar VTP en un switch, realice lo siguiente:

1. En el indicador del modo privilegiado, escriba el comando **configure terminal**.
2. Escriba el comando **vtp mode transparent**.
3. Para regresar al modo privilegiado escriba **end**.
4. Con el comando **show vtp status**, verifique los cambios realizados, después guarde la configuración en el archivo de arranque.

ANEXO

D

RESPUESTA A LAS PREGUNTAS DE REPASO

Capítulo 2

1. Es una red conmutada que está segmentada lógicamente por función, equipo de proyecto o aplicación, sin tener en cuenta la ubicación física de los usuarios en la red. Una VLAN es asociada frecuentemente con subredes IP.
2. VLANs de puerto central, estáticas y dinámicas. En las VLANs de puerto central y estáticas la asignación de los puertos se realiza formando un grupo (dominio de broadcast) en base al identificador o nombre designado para la VLAN. En las VLANs dinámicas la asignación se realiza de manera automática tomando en cuenta la aplicación o el tipo de protocolo y es realizada mediante algún software de administración de red.
3. La tecnología VLAN permite solucionar problemas relacionados con las adiciones, traslados y cambios en la red, Como los usuarios están agrupados lógicamente, las VLANs pueden implementarse independientemente de la localización física y geográfica de estos. Las VLAN incrementan la seguridad de la red.
4. Un enlace de acceso solo es parte de una VLAN, los dispositivos conectados asumen que pertenecen a un dominio broadcast, pero estos no conocen la red física. En cambio, un enlace troncal es una conexión punto a punto que permite transportar tráfico de diversas VLANs en un mismo canal.
5. Es un método de identificación que utilizan los switches para reconocer la pertenencia de las tramas a cierta VLAN y tomar la decisión de envío por la red.
6. ISL y 802.1 Q
7. Conmutación de tramas de datos y mantenimiento de las operaciones de conmutación
8. La conmutación simétrica proporciona anchos de banda de igual capacidad en cualquier puerto del switch, en cambio, la conmutación

asimétrica asigna anchos de banda diferentes, como una combinación de puertos 10/100/1000 Mbps.

9. Es un método de almacenamiento temporal de memoria, que permite a un switch realizar la conmutación de tramas en puertos de diferente capacidad.
10. Almacenamiento y reenvió, y el método de corte; conmutación rápida y conmutación libre de fragmentos.
11. Es una forma de conmutación que permite filtrar los fragmentos de colisión y realizar la detección de errores.
12. Es una dirección lógica que permite la identificación de cualquier dispositivo conectado a una red, está formada de dos partes; un identificador del fabricante y el número de la tarjeta proporcionado por el IEEE.
13. En base a la dirección MAC del equipo conectado en cada uno de los puertos del switch, cuando una trama es recibida, el switch examina la dirección MAC incluida en la trama y la registra en su tabla de direcciones.
14. . El objetivo del protocolo STP es mantener una red libre de bucles
15. Son los puertos que de acuerdo al cálculo del algoritmo STP pueden participar en el envío de datos.
16. La configuración predeterminada de STP, la dirección MAC de cada switch y el número de revisión.

Capítulo 3

1. Realizar la configuración de las interfaces LAN, gestionar los archivos de configuración, controlar y administrar el switch.
2. Modo usuario, privilegiado, modo de configuración global, modo de configuración de control y de interfaz.
3. Comandos globales, comandos de puerto y subcomandos.

4. Los modos usuario, privilegiado y configuración difieren en la cantidad de comandos soportados y el modo de acceso a cada uno, como los comandos varían, cada uno ofrece diferentes opciones de configuración.
5. El IOS del switch ofrece dos métodos de para la configuración de VLANs. El primero, el modo **config-vlan** es utilizado para configurar VLANs en el rango normal utilizando el comando **vlan** en el modo de configuración global, mientras que el segundo, el modo vlan configuration permite la configuración de VLANs en el rango extendido y su acceso de logra desde el modo privilegiado mediante el comando **vlan database.**
6. El procedimiento para solicitar ayuda en cualquier modo de configuración es el mismo, la diferencia radica en la cantidad de comandos a los cuales se puede hacer referencia para realizar alguna consulta.
7. Ayuda relativa al contexto, mensajes de error de consola y el búfer de historial de comandos.
8. Los tipos de ayuda relativa al contexto son la ayuda de texto y ayuda relativa a la sintaxis de un comando.
9. Las funciones administrativas que puede configurar en un switch son el nombre del equipo (hostname), mensajes (Banners), contraseñas (password)y descripción de las interfaces.
10. Contraseñas para el acceso al modo privilegiado y contraseñas para restringir el acceso al modo usuario a través del puerto de consola o mediante el terminal virtual.

Capítulo 4

1. Consultar el número de VLANs soportadas por el switch, determinar si la VLAN pertenecerá al rango normal ó extendido, decidir si utilizará VTP para mantener de manera coherente la configuración de la red.
2. las VLANs son asociadas con subredes IP debido a que crean dominios de difusión y de broadcast agrupados en base al direccionamiento lógico necesario para permitir la comunicación entre estos dominios.
3. **Static-access**. En este tipo de puertos la asignación a una VLAN se hace manualmente. Este modo no requiere de los servicios proporcionados por VTP. Si no es necesario que la información que procesa este protocolo sea difundida por la red, entonces, deberá ajustar VTP al modo transparente. **802.1Q** .Con este modo un puerto de enlace troncal será miembro de todas la VLANs, incluyendo las del rango extendido. Sin embargo, la membresía puede limitarse al configurar una lista de VLANs permitidas en algún puerto. **Dynamic access**. La membresía para configurar un puerto con acceso dinámico está reservada para VLANs configuradas en el rango normal y es asignada en forma dinámica por un VLAN Management Policy Server (VMPS). **Voice VLAN**. Un puerto que trasporte voz en una VLAN, es un puerto de acceso al cual se conectará un teléfono IP de Cisco o algún otro fabricante.

4. El tipo de identificador designado para cada rango, además la configuración de VLANs en rango normal es almacenada en la en la VNRAM, mientras que las VLANs en el rango extendido no.

5. Resulta importante configurar VTP debido a que este protocolo permite que las tramas pertenecientes e determinada VLAN

puedan comunicarse a travez de uno ó varios canales, además, VTP reduce de manera significativa la labor de administración de la red ya que mantiene una configuración coherente después de realizar cambios en la topología de la red.

6. El identificador y nombre de la VLAN, estado, seguridad, MTU, entre otros.

7. Cuando non existen STPs disponibles en el switch y crea una nueva VLAN, STP permanecerá inactivo para esta VLAN y aquellas que sean configuradas posteriormente, dejando de esta manera la red susceptible a loops.

8. La información en la base de datos es ignorada por el switch y esté utilizará la información VLAN o VTP que se encuentre en el archivo de arranque.
9. Los comandos más utilizados para realizar realizar la consulta de VLANs son show vlan y show vlan brief, la diferencia que existe entre ellos es que primero proporciona información más detallada de la configuración en comparación con el segundo.
10. El switch utiliza el nombre de dominio y modo VTP que encuentre en la base de datos.
11. Cuando crea VLANs en el rango extendido debe configurar primero VTP al modo transparente, es decir debe deshabilitarlo, de lo contrario no podrá realizar la configuración.
12. La VLAN es eliminada de la base de datos, pero los Puertos asignados a está, en caso de haberlos, permanecerán inactivos hasta que sean reasignados a otra VLAN o sean reconfigurados a su estado predeterminado.

13. El nombre e identificador de la VLAN, estado, unidad máxima de transmisión, identificadores de seguridad, puente de transición y sesiones SPAN.
14. La VLAN de administración, también conocida como la VLAN natural del switch, permite administrar los cambios relacionados con la configuración.
15. En una VLAN, los host pertenecen a un solo dominio de broadcast, los cuales dividen el flujo de tramas en base a la información de capa 2. Esta capacidad permite que los host host que son mienbros de la misma VLAN podrán comunicarse. Para permitir que la comunicación entre VLANs sea posible, se necesita de un router o switch que soporte funciones a nivel capa 3.

Capítulo 5

1. Es una conexión punto a punto entre una o más interfaces Ethernet de un switch a otro switch o router, los enlaces troncales transportan tramas de múltiples VLANs sobre una sola conexión. Esto permite difundir la VLAN por toda la red.
2. Modo access, dynamic desirable, trunk y nonegotiate.
3. Es un protocolo punto a punto encargado de la negociación de una interfaz que trata de configurarse como enlace troncal.
4. Los dos métodos de etiquetado son ISL y 802.1 Q, el primero es un protocolo propietario de Cisco, el cuál modifica el encabezado de la trama de Ethernet para la identificación de VLANs, mientras que el segundo es un protocolo libre publicado por el IEEE.
5. Los modos soportados por el VTP son; cliente, servidor y transparente.
6. Para configurar un puerto del switch como enlace troncal debe; seleccionar la interfaz, ingresar el comando switchport mode y seleccionar la opción puerto troncal.

7. Los modos VTP validos para que un puerto del switch funcione como puerto troncal son cliente y servidor.
8. Los servidores VTP pueden crear, modificar y eliminar la VLAN y los parámetros de configuración de VLAN de todo un dominio. Los servidores VTP guardan la información de la configuración VLAN en la NVRAM del switch. Los servidores VTP envían mensajes VTP a través de todos los puertos de enlace troncal.
9. Para configurar un puerto como enlace troncal debe seleccionar una interfaz 100/1000 Mbps.

BIBLIOGRAFIA

Creación de Redes Cisco Escalables
Catherine Paquet y Diane Teare
Pearson Educación, Madrid 2001
ISBN: 8420531855

Academia de Networking de Cisco Systems CCNA 3 y 4
Guia del Segundo Año 3ª edición
Cisco Press
ISBN: 8420540803

http://www.cisco.com/en/US/docs/switches/lan/catalyst2950/software/release/12.1_14_ea1/configuration/guide/swvlan.html

VLANs And TRUNKING
http://www.ciscopress.com/articles/